3CORP Technology

PROPOSTA COMERCIAL

PROPOSTA COMERCIAL – 3CORP_V1 2

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO

PE – 020/22 – Processo nº E-20/001.001010/2021

3CORP Technology

Santana de Parnaíba, 11 de Outubro de 2022

A
DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO
Avenida Marechal Câmara, 314, - Bairro Centro, Rio de Janeiro/RJ, CEP 20020-080
A/c: Sr(a). Pregoeiro(a) e Equipe de Apoio

Ref.: **Pregão Eletrônico nº:** 020/22 **Processo nº** E-20/001.001010/2021
Data de Abertura: 11/10/2022 às 11h00min
Objeto: CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DO SERVIÇO DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM, SOB DEMANDA, INCLUINDO OS RECURSOS DE ACESSO AO SERVIÇO DE TELEFONIA FIXA COMUTADA (STFC), NAS MODALIDADES LOCAL, LONGA DISTÂNCIA NACIONAL E INTERNACIONAL. SERVIÇO DE 0800 PARA RECEBIMENTO DE LIGAÇÕES GRATUITAS (LOCAL E DDD) E TRIDÍGITO 129 RESERVADO PARA AS DEFENSORIAS PÚBLICAS. INCLUINDO OS SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO, SUPORTE, MANUTENÇÃO, TREINAMENTO, BEM COMO O FORNECIMENTO DE LINKS, GATEWAYS, ATAS, TELEFONES IP, ENTRE OUTROS EQUIPAMENTOS NECESSÁRIOS PARA O FUNCIONAMENTO DOS SERVIÇOS CONTRATADOS, CONFORME ESPECIFICAÇÕES CONSTANTES NO TERMO DE REFERÊNCIA, CUJAS ESPECIFICAÇÕES TÉCNICAS, QUANTIDADES E DEMAIS CONDIÇÕES SE ENCONTRAM DETALHADOS NO PRESENTE DOCUMENTO.

Prezados Senhores,

Através deste documento, a 3CORP Technology têm como objetivo fornecer informações técnicas referentes à PRESTAÇÃO DO SERVIÇO DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM.

Esta proposta tem como objetivo prover informações que possibilitem o entendimento da solução técnica e funcionalidades que devem ser entregues, e adicionalmente a descrição do nosso plano para prestação de serviços.

A seguir apresentamos detalhes sobre os produtos envolvidos, preços, de acordo com as características técnicas dos equipamentos propostos para o projeto.

Colocando-nos à inteira disposição para quaisquer esclarecimentos adicionais que se fizerem necessários.

Este documento é de responsabilidade da 3CORP Technology não sendo permitido o uso sem autorização prévia e por escrito.

04.238.297/0001-89
3CORP TECHNOLOGY
INFRAESTRUTURA DE TELECOM LTDA
Alameda Oceania, Nº 56,
Polo Empresarial
Tamboré - CEP: 06.543-308
Santana de Parnaiba - SP

3

1. Sobre a 3CORP

A 3CORP Technology é uma empresa brasileira com 20 anos no mercado e é voltada para a entrega das melhores e mais avançadas soluções de Infraestrutura de TI & Telecom. A 3CORP atua como Value Added Partner da Huawei Enterprise, Premium Business Partner da Alcatel-Lucent Enterprise, Microsoft Gold Partner na competência Communications, parceira Enghouse Networks, Hikvision e Vocale Solutions.

A empresa possui uma gama diversificada de clientes nos segmentos financeiros, de governos, indústrias, hotéis, hospitais, serviços e conta com uma equipe de profissionais altamente qualificados nas áreas comercial, técnica e de desenvolvimento voltadas a criar, prover, implementar e dar suporte de acordo com a necessidade dos clientes.

Com atuação nacional, a 3CORP está com sua sede em Alphaville, Santana de Parnaíba, SP, onde funciona toda parte de Logística, Centro de Distribuição, Laboratório Técnico, Network Operations Center (NOC) e Administração Geral. A empresa conta também, com unidades em Brasília e Rio de Janeiro.

2. Objetivo

CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DO SERVIÇO DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM, SOB DEMANDA, INCLUINDO OS RECURSOS DE ACESSO AO SERVIÇO DE TELEFONIA FIXA COMUTADA (STFC), NAS MODALIDADES LOCAL, LONGA DISTÂNCIA NACIONAL E INTERNACIONAL. SERVIÇO DE 0800 PARA RECEBIMENTO DE LIGAÇÕES GRATUITAS (LOCAL E DDD) E TRIDÍGITO 129 RESERVADO PARA AS DEFENSORIAS PÚBLICAS. INCLUINDO OS SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO, SUPORTE, MANUTENÇÃO, TREINAMENTO, BEM COMO O FORNECIMENTO DE LINKS, GATEWAYS, ATAS, TELEFONES IP, ENTRE OUTROS EQUIPAMENTOS NECESSÁRIOS PARA O FUNCIONAMENTO DOS SERVIÇOS CONTRATADOS, CONFORME ESPECIFICAÇÕES CONSTANTES NO TERMO DE REFERÊNCIA, CUJAS ESPECIFICAÇÕES TÉCNICAS, QUANTIDADES E DEMAIS CONDIÇÕES SE ENCONTRAM DETALHADOS NO PRESENTE DOCUMENTO.

3. Dos Serviços

A 3CORP Technology é um parceiro Alcatel-Lucent - "Expert Business Partner" em Business Telephony Unified communications, Collaboration/Conferencing, bem como "Value Added Partner da Huawei Technologies" e possuindo as certificações e capacitações necessárias para implementação e suporte da solução proposta.

São Paulo
Al. Oceânia, 56, Polo Empresarial
Tamboré - Santana de Parnaíba
CEP: 06.543-308
www.3corp.com.br

Resende
Av. Dr. Tácito Vianna Rodrigues,
Nº 300, Galpão 07, Paraíso
CEP 27.536-000
www.3corp.com.br

Brasília
SCN QD 4 BL B Nº 100 Sl 1201
Brasília Empresarial Varig
CEP: 70.714-900
www.3corp.com.br

4. Condições Comerciais

	SERVIÇO PÚBLICO ESTADUAL PROPOSTA DETALHE	ANEXO II **Licitação por Pregão Eletrônico nº 020/22,** **A Realizar-se: 11/10/2022, às 11h** **Requisição nº - PES 0066/2022, PES 0067/2022 e PES 0068/2022.** **Processo nº E-20/001.001010/2021**
	A firma ao lado mencionada propõe fornecer à DPRJ, pelos preços abaixo assinalados, obedecendo rigorosament e às condições est ipuladas const antes do EDITAL.	04.238.297/0001-89 3CORP TECHNOLOGY INFRAESTRUTURA DE TELECOM LTDA Alameda Oceania, Nº 56, Polo Empresarial Tamboré - CEP: 06.543-308 Santana de Parnaiba - SP

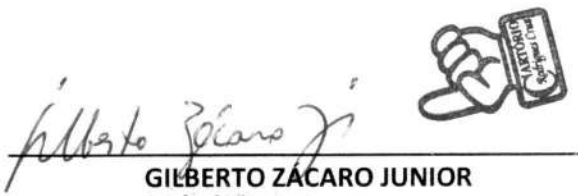
LOTE	ITEM	NÚMERO DE ESTOQUE (ID SIGA)	ESPECIFICAÇÃO	UNID.	QTD	PERÍODO	PREÇO COM ICMS(R$)			PREÇO SEM ICMS (R$)		
							UNIT.	MENSAL	TOTAL	UNIT.	MENSAL	TOTAL

1	1	0477.001.0002 (ID - 176309)	SERVICO TELEFONICO FIXO COMUTADO (STFC) LOCAL COMUTADO COM CENTRAL VIRTUAL,DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM - RAMAL TIPO I Complemento: RAMAL TIPO 1 FRANQUIA ILIMITADA E APARELHO IP TIPO 1 VALOR UNITÁRIO R$: VALOR TOTAL R$:	Unidade	3000	24 (VINTE E QUATRO) MESES	R$ 80,00	R$ 240.000,00	R$ 5.760.000,00	R$ 76,80	R$ 230.400,00	R$ 5.529.600,00
1	2	0477.001.0003 (ID - 176310)	SERVICO TELEFONICO FIXO COMUTADO (STFC) LOCAL COMUTADO COM CENTRAL VIRTUAL,DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM (RAMAL TIPO II) Complemento: RAMAL TIPO 2 FRANQUIA ILIMITADA E APARELHO IP TIPO 2 VALOR UNITÁRIO R$: VALOR TOTAL R$:	Unidade	1150	24 (VINTE E QUATRO) MESES	R$ 165,00	R$ 189.750,00	R$ 4.554.000,00	R$ 158,40	R$ 182.160,00	R$ 4.371.840,00

3CORP Technology
São Paulo
Al. Oceânia, 56, Polo Empresarial Tamboré - Santana de Parnaíba
CEP: 06.543-308
www.3corp.com.br
Resende
Av. Dr. Tácito Vianna Rodrigues, Nº 300, Galpão 07, Paraíso
CEP 27.536-000
www.3corp.com.br
Brasília
SCN QD 4 BL B Nº 100 Sl 1201, Brasília Empresarial Varig
CEP: 70.714-900
www.3corp.com.br

1	3	0477.001.0004 (ID - 176311)	SERVICO TELEFONICO FIXO COMUTADO (STFC) LOCAL COMUTADO COM CENTRAL VIRTUAL,DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM E FORNECIMENTO DE SOFTPHONE MOBILE VALOR UNITÁRIO R$: VALOR TOTAL R$:	Unidade	900	24 (VINTE E QUATRO) MESES	R$ 27,00	R$ 24.300,00	R$ 583.200,00	R$ 25,92	R$ 23.328,00	R$ 559.872,00
1	4	0218.001.0001 (ID - 176308)	SERVICO TELEFONICO FIXO COMUTADO (STFC) - LONGA DISTANCIA INTERNACIONAL (LDI),DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA DE LDI (FIXO-FIXO E FIXO-MOVEL) Complement o: LIGAÇÃO LONGA DISTÂNCIA INTERNACIONAL FIXO-FIXO / FIXO-MÓVEL VALOR UNITÁRIO R$: VALOR TOTAL R$: VALOR GLOBAL R$:	Minuto	200	24 (VINTE E QUATRO) MESES	R$ 14,00	R$ 2.800,00	R$ 2.800,00	R$ 13,44	R$ 2.688,00	R$ 64.512,00

	Observações **1ª A PROPOSTA DETALHE deverá:** **- ser preenchida integralment e por processo mecânico ou eletrônico, sem emendas e rasuras;** **- conter os preços em algarismos por extenso, por unidade, já incluídas as despesas de fretes, impostos federais ou estaduais e descontos especiais.** **2ª – O proponente se obrigará, mediante devolução da PROPOSTA DETALHE, a cumprir os termos nela contidos.** **3ª – As duas primeiras vias da PROPOSTA DETALHE deverão ser devolvidas a este órgão, até à hora e data marcadas em envelope fechado, com indicação do seu número e data do encerramento.** **4ª – A licitação mediante PROPOSTA DETALHE poderá ser anulada no todo, ou em parte, de conformidade com a legislação vigente.** **5ª – Caso o Termo de Referência cont enha anexo específico relativo à Propost a Detalhe, este deverá ser apresent ado juntamente com o presente Anexo II.**	**Prazo de execução: De acordo com o Termo de Referência** **Validade da Proposta - Detalhe: preços válidos por 60 (sessenta) dias úteis.** **Local de entrega/execução: conforme o Termo de Referência.** **Declaramos inteira submissão ao presente termo e legislação vigente.** **Em 11/10/2022**

DATA 11/10/2022	 **GILBERTO ZACARO JUNIOR** **SÓCIO - DIRETOR** **RG: 13.189.904-1 SSP/SP** **CPF: 043.669.268.65** **3CORP TECHNOLOGY** **INFRAESTRUTURA DE TELECOM LTDA**

IDENTIFICAÇÃO DA EMPRESA LICITANTE:		
RAZÃO SOCIAL: 3CORP TECHNOLOGY INFRAESTRUTURA DE TELECOM LTDA		
CNPJ: 04.238.297/0001-89		
ENDEREÇO COMPLETO: Alameda Oceania, nº 56 - Polo Empresarial, Tamboré - Santana de Parnaíba/SP		
CEP: 06.543-308	**FONE:** (11) 4450-6075	**E-MAIL:** Governo@3corp.com.br
DADOS BANCÁRIOS		
Agência: 3348-0	**Conta-Corrente:** 61868-3	**Banco:** Banco do Brasil - 001

CARTÓRIO Rodrigues Cruz

1º TABELIÃO DE NOTAS E DE PROTESTO DE LETRAS E TÍTULOS

Antonio Augusto Rodrigues Cruz - Tabelião

CEP 06501-130 - Rua Pedro Procópio, 118 - Ed. Lázara Rodrigues Cruz - Santana de Parnaíba/SP
Tel.: (11) 4622-7700 - www.cartoriorodriguescruz.com.br - cartorio@cartoriorodriguescruz.com.br

Reconheço por SEMELHANÇA a(s) Firma(s) de: GILBERTO ZACARO JUNIOR. Dou fé.
Santana de Parnaíba/SP, 13/10/2022. Em Test. _____ da verdade.
LARISSA DOS SANTOS SILVA - ESCREVENTE.
Etiqueta: 770906 Feita por: ANA CARLA Total R$ 7,43
Selos: AA 950895

Colégio Notarial do Brasil Seção São Paulo ARPEN SP
118802
FIRMA 1
S10926AA0950895

1º TABELIÃO DE NOTAS E DE PROTESTO DE LETRAS E TÍTULOS SANTANA DE PARNAÍBA SP
CARTÓRIO Rodrigues Cruz
Antonio Augusto Rodrigues Cruz

	Observações **1ª A PROPOSTA DETALHE deverá:** **- ser preenchida integralment e por processo mecânico ou eletrônico, sem emendas e rasuras;** **- conter os preços em algarismos por extenso, por unidade, já incluídas as despesas de fretes, impostos federais ou estaduais e descontos especiais.** **2ª – O proponente se obrigará, mediante devolução da PROPOSTA DETALHE, a cumprir os termos nela contidos.** **3ª – As duas primeiras vias da PROPOSTA DETALHE deverão ser devolvidas a este órgão, até à hora e data marcadas em envelope fechado, com indicação do seu** **número e data do encerramento.** **4ª – A licitação mediante PROPOSTA DETALHE poderá ser anulada no todo, ou em parte, de conformidade com a legislação vigente.** **5ª – Caso o Termo de Referência cont enha anexo específico relativo à Propost a Detalhe, este deverá ser apresent ado juntamente com o presente Anexo II.**	**Prazo de execução: De acordo com o Termo de Referência** **Validade da Proposta - Detalhe: preços válidos por 60 (sessenta) dias úteis.** **Local de entrega/execução: conforme o Termo de Referência.** **Declaramos inteira submissão ao presente termo e legislação vigente.** **Em 11/10/2022.**

VALOR TOTAL DA PROPOSTA: R$ 10.900.000,00 (Dez milhões, e novecentos mil reais.)

LOTE	ITEM	ESPECIFICAÇÃO	MARCA	MODELO
1	1	SERVICO TELEFONICO FIXO COMUTADO (STFC) LOCAL COMUTADO COM CENTRAL VIRTUAL,DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM - RAMAL TIPO I Complemento: RAMAL TIPO 1 FRANQUIA ILIMITADA E APARELHO IP TIPO 1 VALOR UNITÁRIO R$: VALOR TOTAL R$:	Alcatel-Lucent	OpenTouch Enterprise Cloud - SIP Premium User
			Alcatel-Lucent	Rainbow
			Alcatel-Lucent	M7 DeskPhone
1	2	SERVICO TELEFONICO FIXO COMUTADO (STFC) LOCAL COMUTADO COM CENTRAL VIRTUAL,DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM (RAMAL TIPO II) Complemento: RAMAL TIPO 2 FRANQUIA ILIMITADA E APARELHO IP TIPO 2 VALOR UNITÁRIO R$: VALOR TOTAL R$:	Alcatel-Lucent	OpenTouch Enterprise Cloud - SIP Premium User
			Alcatel-Lucent	Rainbow
			Alcatel-Lucent	8088 Smart Deskphone
1	3	SERVICO TELEFONICO FIXO COMUTADO (STFC) LOCAL COMUTADO COM CENTRAL VIRTUAL,DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM E FORNECIMENTO DE SOFTPHONE MOBILE VALOR UNITÁRIO R$: VALOR TOTAL R$:	Alcatel-Lucent	Rainbow
1	4	SERVICO TELEFONICO FIXO COMUTADO (STFC) - LONGA DISTANCIA INTERNACIONAL (LDI),DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA DE LDI (FIXO-FIXO E FIXO-MOVEL) Complement o: LIGAÇÃO LONGA DISTÂNCIA INTERNACIONAL FIXO-FIXO / FIXO-MÓVEL VALOR UNITÁRIO R$: VALOR TOTAL R$: VALOR GLOBAL R$:	3CORP	3CORP

CONDIÇÕES GERAIS/DADOS DA LICITANTE:

Prazo de pagamento: 30 (trinta) dias a contar do recebimento da nota fiscal/fatura pela equipe de fiscalização do contrato.

Prazo de Validade: 60 (sessenta) dias contados da data de abertura da sessão, conforme disposto no item 3.

Prazo de Entrega/Instalação: 90 (noventa) dias corridos após o recebimento da ordem de serviços emitida pela Fiscalização.

Local de Entrega: Conforme edital.

DADOS PARA ASSINATURA DO CONTRATO (ASSINAM EM CONJUNTO):

Nome: GIUSEPPE FORESTIERO Data de Nascimento: 11/09/1960 Nacionalidade: brasileiro Cargo: Presidente Profissão: Economista Estado Civil: Casado CPF: 989.128.018-72 RG: 13.023.683-4 SSP/SP e-mail: governo@3corp.com.br Telefones: 11 3056-7733/11 4118-2700 Endereço (domicílio): Alameda Suiça, 90 Alphaville Residencial Um – Barueri/SP CEP 06474-220	Nome: GILBERTO ZÁCARO JUNIOR Data de Nascimento: 21/12/1964 Nacionalidade: brasileiro Cargo: Diretor Profissão: Administrador Estado Civil: Casado CPF: 043.669.268-65 RG: 13.189.904-1SSP/SP e-mail: governo@3corp.com.br Telefones: 11 3056-7733/11 4118-2700 Endereço (domicílio): Praça Oiapoque, AP 503 - Alphaville Industrial - Barueri - SP, 06454-060

12

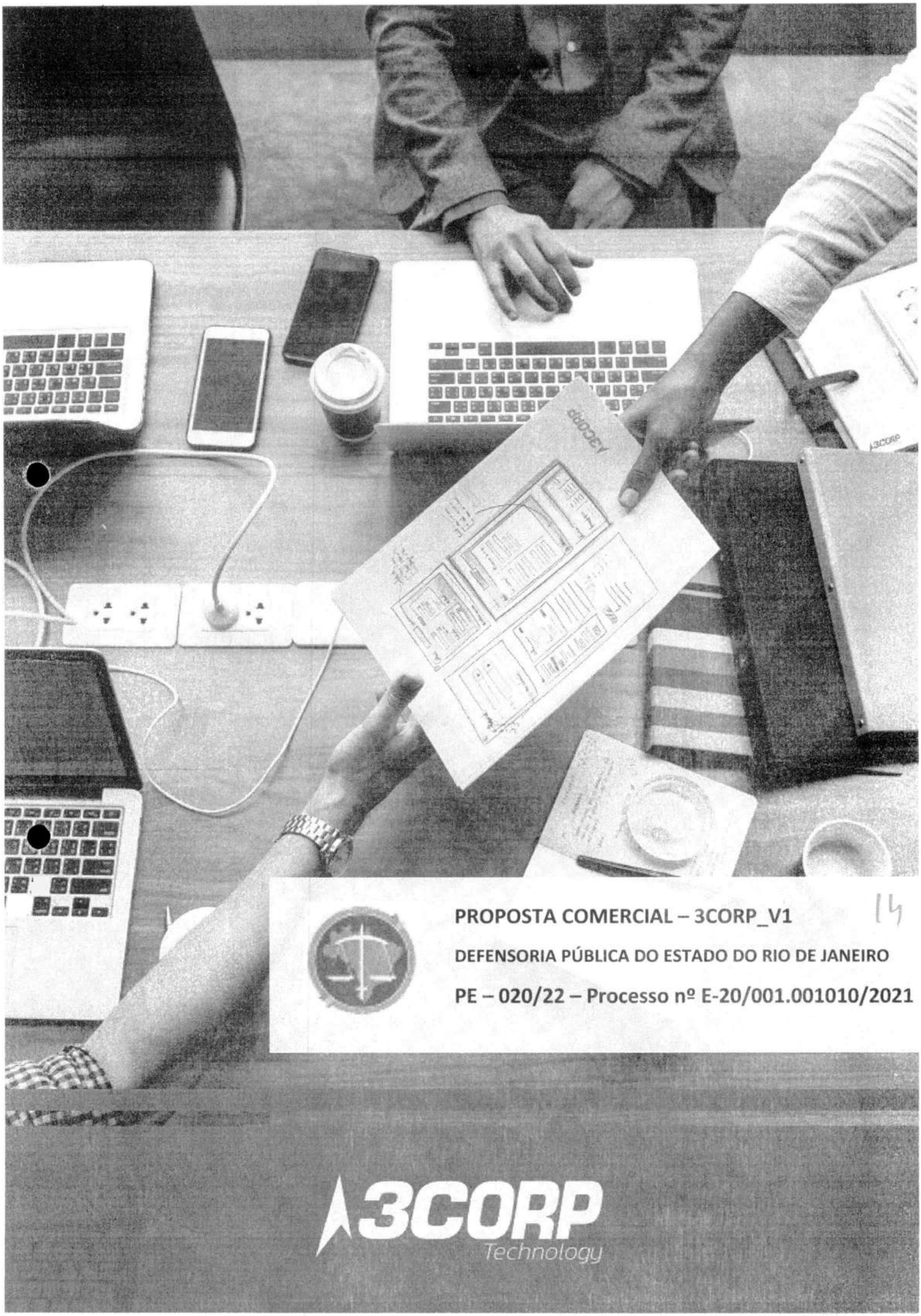
3CORP Technology

04.238.297/0001-89

3CORP TECHNOLOGY
INFRAESTRUTURA DE TELECOM LTDA

Alameda Oceania, Nº 56,
Polo Empresarial
Tamboré - CEP: 06.543-308
Santana de Parnaiba - SP

13



PROPOSTA COMERCIAL – 3CORP_V1 14

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO

PE – 020/22 – Processo nº E-20/001.001010/2021

3CORP Technology

Santana de Parnaíba, 11 de Outubro de 2022

A
DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO
Avenida Marechal Câmara, 314, - Bairro Centro, Rio de Janeiro/RJ, CEP 20020-080
A/c: Sr(a). Pregoeiro(a) e Equipe de Apoio

Ref.: **Pregão Eletrônico nº:** 020/22 **Processo nº** E-20/001.001010/2021
Data de Abertura: 11/10/2022 às 11h00min
Objeto: CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DO SERVIÇO DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM, SOB DEMANDA, INCLUINDO OS RECURSOS DE ACESSO AO SERVIÇO DE TELEFONIA FIXA COMUTADA (STFC), NAS MODALIDADES LOCAL, LONGA DISTÂNCIA NACIONAL E INTERNACIONAL. SERVIÇO DE 0800 PARA RECEBIMENTO DE LIGAÇÕES GRATUITAS (LOCAL E DDD) E TRIDÍGITO 129 RESERVADO PARA AS DEFENSORIAS PÚBLICAS. INCLUINDO OS SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO, SUPORTE, MANUTENÇÃO, TREINAMENTO, BEM COMO O FORNECIMENTO DE LINKS, GATEWAYS, ATAS, TELEFONES IP, ENTRE OUTROS EQUIPAMENTOS NECESSÁRIOS PARA O FUNCIONAMENTO DOS SERVIÇOS CONTRATADOS, CONFORME ESPECIFICAÇÕES CONSTANTES NO TERMO DE REFERÊNCIA, CUJAS ESPECIFICAÇÕES TÉCNICAS, QUANTIDADES E DEMAIS CONDIÇÕES SE ENCONTRAM DETALHADOS NO PRESENTE DOCUMENTO.

Prezados Senhores,

Através deste documento, a 3CORP Technology têm como objetivo fornecer informações técnicas referentes à PRESTAÇÃO DO SERVIÇO DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM.

Esta proposta tem como objetivo prover informações que possibilitem o entendimento da solução técnica e funcionalidades que devem ser entregues, e adicionalmente a descrição do nosso plano para prestação de serviços.

A seguir apresentamos detalhes sobre os produtos envolvidos, preços, de acordo com as características técnicas dos equipamentos propostos para o projeto.

Colocando-nos à inteira disposição para quaisquer esclarecimentos adicionais que se fizerem necessários.

Este documento é de responsabilidade da 3CORP Technology não sendo permitido o uso sem autorização prévia e por escrito.

04.238.297/0001-89
3CORP TECHNOLOGY
INFRAESTRUTURA DE TELECOM LTDA
Alameda Oceania, Nº 56,
Polo Empresarial
Tamboré - CEP: 06.543-308
Santana de Parnaíba - SP

15

1. Sobre a 3CORP

A 3CORP Technology é uma empresa brasileira com 20 anos no mercado e é voltada para a entrega das melhores e mais avançadas soluções de Infraestrutura de TI & Telecom. A 3CORP atua como Value Added Partner da Huawei Enterprise, Premium Business Partner da Alcatel-Lucent Enterprise, Microsoft Gold Partner na competência Communications, parceira Enghouse Networks, Hikvision e Vocale Solutions.

A empresa possui uma gama diversificada de clientes nos segmentos financeiros, de governos, indústrias, hotéis, hospitais, serviços e conta com uma equipe de profissionais altamente qualificados nas áreas comercial, técnica e de desenvolvimento voltadas a criar, prover, implementar e dar suporte de acordo com a necessidade dos clientes.

Com atuação nacional, a 3CORP está com sua sede em Alphaville, Santana de Parnaíba, SP, onde funciona toda parte de Logística, Centro de Distribuição, Laboratório Técnico, Network Operations Center (NOC) e Administração Geral. A empresa conta também, com unidades em Brasília e Rio de Janeiro.

2. Objetivo

CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DO SERVIÇO DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM, SOB DEMANDA, INCLUINDO OS RECURSOS DE ACESSO AO SERVIÇO DE TELEFONIA FIXA COMUTADA (STFC), NAS MODALIDADES LOCAL, LONGA DISTÂNCIA NACIONAL E INTERNACIONAL. SERVIÇO DE 0800 PARA RECEBIMENTO DE LIGAÇÕES GRATUITAS (LOCAL E DDD) E TRIDÍGITO 129 RESERVADO PARA AS DEFENSORIAS PÚBLICAS. INCLUINDO OS SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO, SUPORTE, MANUTENÇÃO, TREINAMENTO, BEM COMO O FORNECIMENTO DE LINKS, GATEWAYS, ATAS, TELEFONES IP, ENTRE OUTROS EQUIPAMENTOS NECESSÁRIOS PARA O FUNCIONAMENTO DOS SERVIÇOS CONTRATADOS, CONFORME ESPECIFICAÇÕES CONSTANTES NO TERMO DE REFERÊNCIA, CUJAS ESPECIFICAÇÕES TÉCNICAS, QUANTIDADES E DEMAIS CONDIÇÕES SE ENCONTRAM DETALHADOS NO PRESENTE DOCUMENTO.

3. Dos Serviços

A 3CORP Technology é um parceiro Alcatel-Lucent - "Expert Business Partner" em Business Telephony Unified communications, Collaboration/Conferencing, bem como "Value Added Partner da Huawei Technologies" e possuindo as certificações e capacitações necessárias para implementação e suporte da solução proposta.

16

4. Condições Comerciais

<table>
<tr><td></td><td colspan="3">SERVIÇO PÚBLICO ESTADUAL
PROPOSTA DETALHE</td><td colspan="9">ANEXO II
Licitação por Pregão Eletrônico nº 020/22,
A Realizar-se: 11/10/2022, às 11h
Requisição nº - PES 0066/2022, PES 0067/2022 e PES 0068/2022.
Processo nº E-20/001.001010/2021</td></tr>
<tr><td></td><td colspan="3">**A firma ao lado mencionada propõe fornecer à DPRJ, pelos preços abaixo assinalados, obedecendo rigorosament e às condições est ipuladas const antes do EDITAL.**</td><td colspan="9">04.238.297/0001-89
3CORP TECHNOLOGY
INFRAESTRUTURA DE TELECOM LTDA
Alameda Oceania, Nº 56,
Polo Empresarial
Tamboré - CEP: 06.543-308
Santana de Parnaiba - SP</td></tr>
<tr><td rowspan="2">LOTE</td><td rowspan="2">ITEM</td><td rowspan="2">NÚMERO DE ESTOQUE (ID SIGA)</td><td rowspan="2">ESPECIFICAÇÃO</td><td rowspan="2">UNID.</td><td rowspan="2">QTD</td><td rowspan="2">PERÍODO</td><td colspan="3">PREÇO COM ICMS(R$)</td><td colspan="3">PREÇO SEM ICMS (R$)</td></tr>
<tr><td>UNIT.</td><td>MENSAL</td><td>TOTAL</td><td>UNIT.</td><td>MENSAL</td><td>TOTAL</td></tr>
</table>

1	1	0477.001.0002 (ID - 176309)	SERVICO TELEFONICO FIXO COMUTADO (STFC) LOCAL COMUTADO COM CENTRAL VIRTUAL,DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM - RAMAL TIPO I Complemento: RAMAL TIPO 1 FRANQUIA ILIMITADA E APARELHO IP TIPO 1 VALOR UNITÁRIO R$: VALOR TOTAL R$:	Unidade	3000	24 (VINTE E QUATRO) MESES	R$ 80,00	R$ 240.000,00	R$ 5.760.000,00	R$ 76,80	R$ 230.400,00	R$ 5.529.600,00
1	2	0477.001.0003 (ID - 176310)	SERVICO TELEFONICO FIXO COMUTADO (STFC) LOCAL COMUTADO COM CENTRAL VIRTUAL,DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM (RAMAL TIPO II) Complemento: RAMAL TIPO 2 FRANQUIA ILIMITADA E APARELHO IP TIPO 2 VALOR UNITÁRIO R$: VALOR TOTAL R$:	Unidade	1150	24 (VINTE E QUATRO) MESES	R$ 165,00	R$ 189.750,00	R$ 4.554.000,00	R$ 158,40	R$ 182.160,00	R$ 4.371.840,00

18

1	3	0477.001.0004 (ID - 176311)	SERVICO TELEFONICO FIXO COMUTADO (STFC) LOCAL COMUTADO COM CENTRAL VIRTUAL,DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM E FORNECIMENTO DE SOFTPHONE MOBILE VALOR UNITÁRIO R$: VALOR TOTAL R$:	Unidade	900	24 (VINTE E QUATRO) MESES	R$ 27,00	R$ 24.300,00	R$ 583.200,00	R$ 25,92	R$ 23.328,00	R$ 559.872,00
1	4	0218.001.0001 (ID - 176308)	SERVICO TELEFONICO FIXO COMUTADO (STFC) - LONGA DISTANCIA INTERNACIONAL (LDI),DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA DE LDI (FIXO-FIXO E FIXO-MOVEL) Complement o: LIGAÇÃO LONGA DISTÂNCIA INTERNACIONAL FIXO-FIXO / FIXO-MÓVEL VALOR UNITÁRIO R$: VALOR TOTAL R$: VALOR GLOBAL R$:	Minuto	200	24 (VINTE E QUATRO) MESES	R$ 14,00	R$ 2.800,00	R$ 2.800,00	R$ 13,44	R$ 2.688,00	R$ 64.512,00

19

Observações **1ª A PROPOSTA DETALHE deverá:** **- ser preenchida integralment e por processo mecânico ou eletrônico, sem emendas e rasuras;** **- conter os preços em algarismos por extenso, por unidade, já incluídas as despesas de fretes, impostos federais ou estaduais e descontos especiais.** **2ª – O proponente se obrigará, mediante devolução da PROPOSTA DETALHE, a cumprir os termos nela contidos.** **3ª – As duas primeiras vias da PROPOSTA DETALHE deverão ser devolvidas a este órgão, até à hora e data marcadas em envelope fechado, com indicação do seu** **número e data do encerramento.** **4ª – A licitação mediante PROPOSTA DETALHE poderá ser anulada no todo, ou em parte, de conformidade com a legislação vigente.** 5ª – Caso o Termo de Referência cont enha anexo específico relativo à Propost a Detalhe, este deverá ser apresent ado juntamente com o presente Anexo II.	**Prazo de execução: De acordo com o Termo de Referência** **Validade da Proposta - Detalhe: preços válidos por 60 (sessenta) dias úteis.** **Local de entrega/execução: conforme o Termo de Referência.** **Declaramos inteira submissão ao presente termo e legislação vigente.** **Em 11/10/2022.**

VALOR TOTAL DA PROPOSTA: R$ 10.900.000,00 (Dez milhões, e novecentos mil reais.)

	DATA 11/10/2022	 **GILBERTO ZÁCARO JUNIOR** **SÓCIO - DIRETOR** **RG: 13.189.904-1 SSP/SP** **CPF: 043.669.268.65** **3CORP TECHNOLOGY** **INFRAESTRUTURA DE TELECOM LTDA**

IDENTIFICAÇÃO DA EMPRESA LICITANTE:		
RAZÃO SOCIAL: 3CORP TECHNOLOGY INFRAESTRUTURA DE TELECOM LTDA		
CNPJ: 04.238.297/0001-89		
ENDEREÇO COMPLETO: Alameda Oceania, nº 56 - Polo Empresarial, Tamboré - Santana de Parnaíba/SP		
CEP: 06.543-308	**FONE:** (11) 4450-6075	**E-MAIL:** Governo@3corp.com.br
DADOS BANCÁRIOS		
Agência: 3348-0	**Conta-Corrente:** 61868-3	**Banco:** Banco do Brasil - 001

21

CARTÓRIO Rodrigues Cruz

1º TABELIÃO DE NOTAS E DE PROTESTO DE LETRAS E TÍTULOS

Antonio Augusto Rodrigues Cruz - Tabelião

CEP 06501-180 - Rua Pedro Procópio, 118 - Ed. Lázara Rodrigues Cruz - Santana de Parnaíba/SP
Tel.: (11) 4622-7700 - www.cartoriorodriguescruz.com.br - cartorio@cartoriorodriguescruz.com.br

Reconheco por SEMELHANCA a(s) firma(s) de: GILBERTO ZACARO JUNIOR. Dou fe.
Santana de Parnaíba/SP, 13/10/2022. Em Test. _____ da verdade.
LARISSA DOS SANTOS SILVA - ESCREVENTE.
Etiqueta: 776007 Feito por: ANA CARLA Total R$ 7,43
Selos: AA 95089[illegible]

Colégio Notarial do Brasil Seção São Paulo — ARPEN SP
118602
FIRMA 1
S10926AA0950896

1º TABELIÃO DE NOTAS E DE PROTESTO DE LETRAS E TÍTULOS — SANTANA DE PARNAÍBA — SP
CARTÓRIO Rodrigues Cruz
Antonio Augusto Rodrigues Cruz — Tabelião
Lei 8.935 de 18/11/1994 - Regulamenta o Art. 236 da Constituição Federal

LOTE	ITEM	ESPECIFICAÇÃO	MARCA	MODELO
1	1	SERVICO TELEFONICO FIXO COMUTADO (STFC) LOCAL COMUTADO COM CENTRAL VIRTUAL,DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM - RAMAL TIPO I Complemento: RAMAL TIPO 1 FRANQUIA ILIMITADA E APARELHO IP TIPO 1 VALOR UNITÁRIO R$: VALOR TOTAL R$:	Alcatel-Lucent	OpenTouch Enterprise Cloud - SIP Premium User
			Alcatel-Lucent	Rainbow
			Alcatel-Lucent	M7 DeskPhone
1	2	SERVICO TELEFONICO FIXO COMUTADO (STFC) LOCAL COMUTADO COM CENTRAL VIRTUAL,DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM (RAMAL TIPO II) Complemento: RAMAL TIPO 2 FRANQUIA ILIMITADA E APARELHO IP TIPO 2 VALOR UNITÁRIO R$: VALOR TOTAL R$:	Alcatel-Lucent	OpenTouch Enterprise Cloud - SIP Premium User
			Alcatel-Lucent	Rainbow
			Alcatel-Lucent	8088 Smart Deskphone
1	3	SERVICO TELEFONICO FIXO COMUTADO (STFC) LOCAL COMUTADO COM CENTRAL VIRTUAL,DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA IP COM PLATAFORMA DE PABX EM NUVEM E FORNECIMENTO DE SOFTPHONE MOBILE VALOR UNITÁRIO R$: VALOR TOTAL R$:	Alcatel-Lucent	Rainbow
1	4	SERVICO TELEFONICO FIXO COMUTADO (STFC) - LONGA DISTANCIA INTERNACIONAL (LDI),DESCRIÇÃO: CONTRATACAO DE EMPRESA ESPECIALIZADA NA PRESTACAO DE SERVICOS DE TELEFONIA DE LDI (FIXO-FIXO E FIXO-MOVEL) Complement o: LIGAÇÃO LONGA DISTÂNCIA INTERNACIONAL FIXO-FIXO / FIXO-MÓVEL VALOR UNITÁRIO R$: VALOR TOTAL R$: VALOR GLOBAL R$:	3CORP	3CORP

22

CONDIÇÕES GERAIS/DADOS DA LICITANTE:

Prazo de pagamento: 30 (trinta) dias a contar do recebimento da nota fiscal/fatura pela equipe de fiscalização do contrato.

Prazo de Validade: 60 (sessenta) dias contados da data de abertura da sessão, conforme disposto no item 3.

Prazo de Entrega/Instalação: 90 (noventa) dias corridos após o recebimento da ordem de serviços emitida pela Fiscalização.

Local de Entrega: Conforme edital.

DADOS PARA ASSINATURA DO CONTRATO (ASSINAM EM CONJUNTO):

Nome: GIUSEPPE FORESTIERO Data de Nascimento: 11/09/1960 Nacionalidade: brasileiro Cargo: Presidente Profissão: Economista Estado Civil: Casado CPF: 989.128.018-72 RG: 13.023.683-4 SSP/SP e-mail: governo@3corp.com.br Telefones: 11 3056-7733/11 4118-2700 Endereço (domicílio): Alameda Suiça, 90 Alphaville Residencial Um – Barueri/SP CEP 06474-220	Nome: GILBERTO ZÁCARO JUNIOR Data de Nascimento: 21/12/1964 Nacionalidade: brasileiro Cargo: Diretor Profissão: Administrador Estado Civil: Casado CPF: 043.669.268-65 RG: 13.189.904-1SSP/SP e-mail: governo@3corp.com.br Telefones: 11 3056-7733/11 4118-2700 Endereço (domicílio): Praça Oiapoque, AP 503 - Alphaville Industrial - Barueri - SP, 06454-060

23

3CORP Technology

04.238.297/0001-89

3CORP TECHNOLOGY
INFRAESTRUTURA DE TELECOM LTDA

Alameda Oceania, Nº 56,
Polo Empresarial
Tamboré - CEP: 06.543-308
Santana de Parnaiba - SP

24

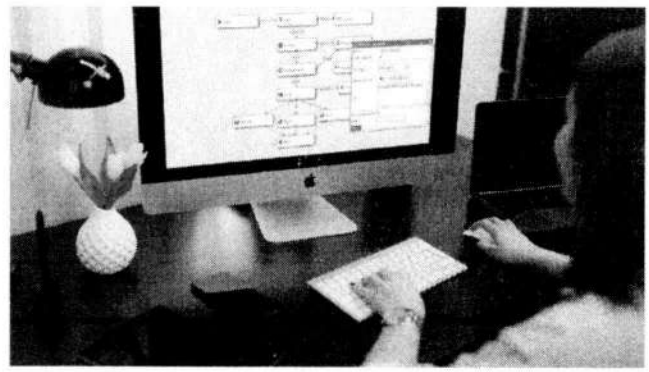
3CORP Technology

CATÁLOGOS

25

Alcatel·Lucent
Enterprise

Alcatel-Lucent Visual Automated Attendant



In business, a telephone call is often the first point of contact. Visual Automated Attendant provides a professional image with a virtual receptionist available 24/7, delivering a quality response to your customers.

Provide your callers a great service experience by starting off with a courteous greeting and routing them directly to employees, departments or voicemail. The programming interface is intuitive with prompts that can be easily customized plus routing rules that instantly adapt to new business needs.

Transform your incoming telephone calls into a sustainable and recurring business relationship. Visual Automated Attendant advanced capabilities offer endless opportunities for a personalized routing and greeting experience for your customers.

Features	Benefits
Present a professional image and response to your customers with automated 24/7 call routing and greeting	• **Easy management of routing script:** Drag and drop building blocks to create call routing based on business hours and calendars • **Prompt upload and recording** anytime and wherever you are. Use a web interface or any phone. • **Direct dial** and **filtering** based on caller and called number providing instant and accurate routing. • **Web interface offering dashboard**, **reporting** and **export** capabilities. • **Text To Speech** (TTS) and **Automatic Speech Recognition** (ASR) for easier customer experience.
Build a recurring business relationship by offering personalized call routing and greeting including integration with the businesses' database or contact center	• **Zero downtime operations**. Update prompts and routing on the go. • Interactive Voice Response (**IVR**) option with **SQL and HTTP connector**. Route calls based on information in your database or suggest satisfaction surveys. • Call Center **integration with Alcatel-Lucent OmniTouch Contact Center Standard Edition**: Qualify calls and collect information to provide a personalized service.
Control and reduce operation costs: The solution offers an intuitive programming interface that anybody can use. The solution is scalable, multi-tenant and SIP-based to offer expert call routing and greeting for small to very large multi-site organizations	• **Intuitive graphical interface**: Minimize training time and required IT skills • **Scalable software** offering **SIP-based connectivity** to communication servers. Unify welcome and reduce operation costs with a centralized routing and greeting solution. • **High-availability**: Load balancing can be provided with the VAA • **Multi-tenant**: Usable by multiple customers each with their own isolated view. • **Delegation**: Different levels of management can be assigned to users.

Figure 1: Example of a routing script configuration via a simple drag and drop of building blocks

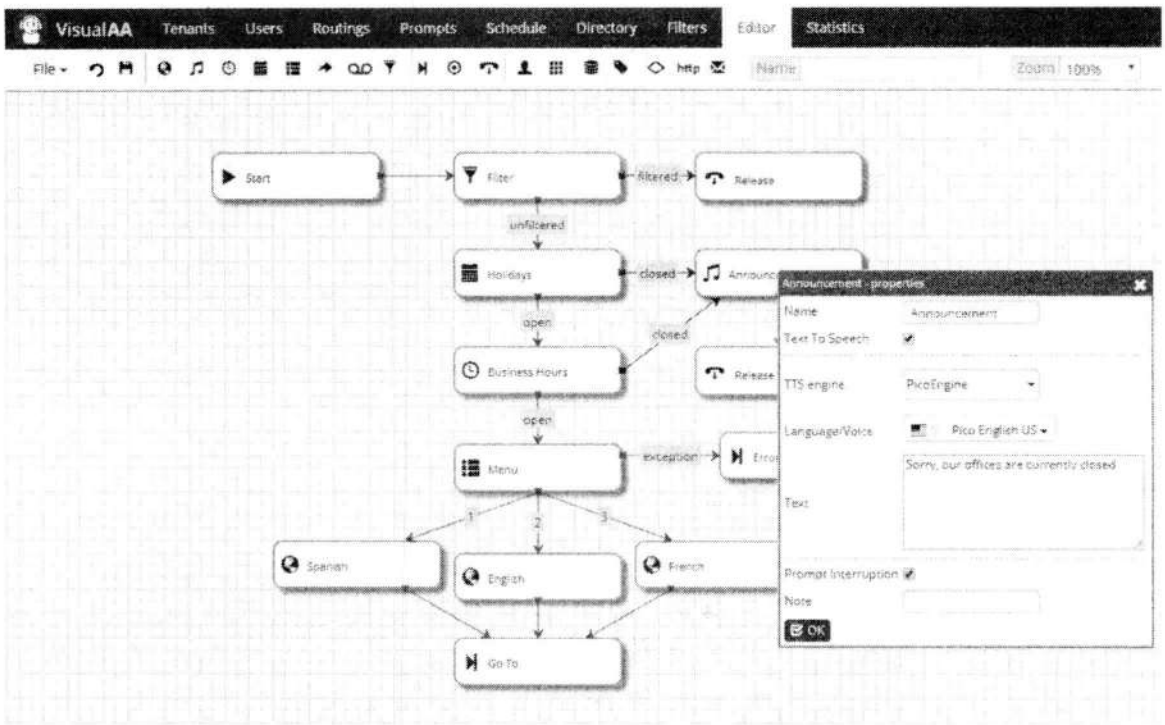
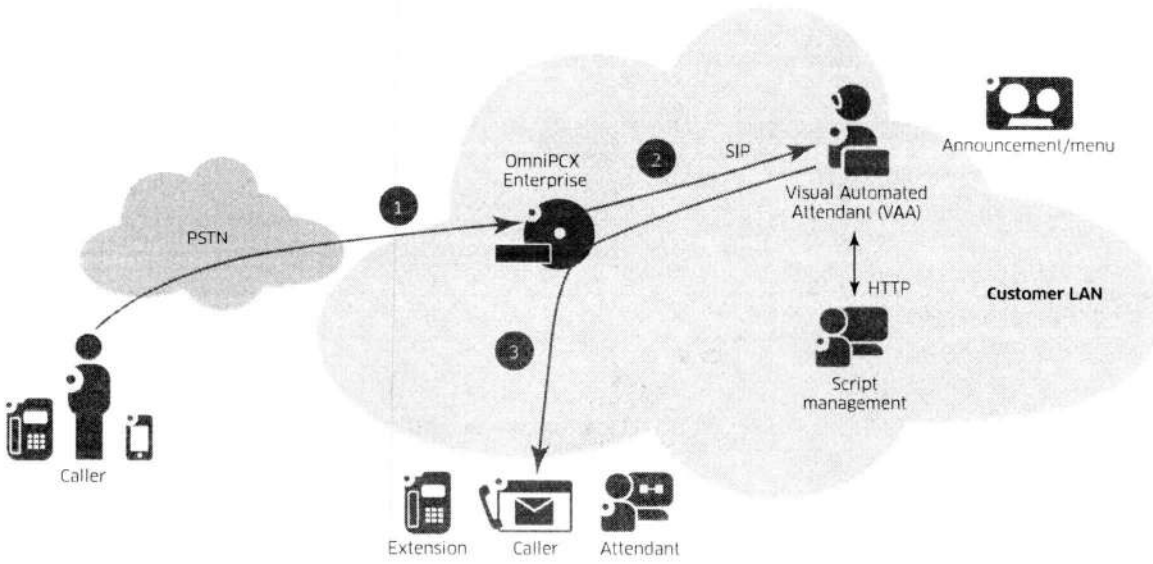


Figure 2: Example of incoming call processing and architecture



1. Incoming call to the welcome number
2. OmniPCX Enterprise CS routes the call to the Visual Automated Attendant using SIP
3. Visual Automated Attendant plays prompts and routes the call back to OmniPCX Enterprise CS.

27

Technical specifications

Software release

- Alcatel-Lucent OmniPCX Enterprise Communication Server: Current supported releases
- Alcatel-Lucent OpenTouch Enterprise Cloud: Current supported releases

Server requirements

- Software delivery on any appliance server:
  - ¬ Suse Linux Enterprise Server
  - ¬ Hardware requirements: Table 1
- Software delivery on VMware vSphere 6.x and 7.x
  - ¬ VMware vSphere delivery and support not included
- Software delivery on HyperV
  - ¬ HyperV on Windows Server 2016
  - ¬ HyperV tools mandatory

Visual script editor

- Web based graphical interface
- Trees: unlimited
- Building blocks (nodes):
  - ¬ Simple drag and drop
  - ¬ Start
  - ¬ Select language
  - ¬ Announcement
  - ¬ Business hours
  - ¬ Calendar
  - ¬ Menu: Up to 12 choices (0-9, #,*)
  - ¬ TTS embedded or connector to cloud provider (Google, IBM Watson)
  - ¬ Transfer: Blind, supervised, dial by name, extension number, prompt interruption, no answer, busy, network error, wrong number conditions
  - ¬ ASR connector to Google
  - ¬ Transfer to voicemail
  - ¬ Filter: On called number, on calling number, regular expression, CSV file import
  - ¬ Go To Tree
  - ¬ Record prompt
  - ¬ Release
- Delegation: Role-based management:
  - ¬ User
  - ¬ Routing
  - ¬ Prompt
  - ¬ Directory
  - ¬ Filter
  - ¬ Calendar
- Multi-tenant management:
  - ¬ Unlimited number of tenants
  - ¬ Isolated view
  - ¬ Script management
  - ¬ Performance reports
- Direct Dial
  - ¬ Prompt interruption and direct key in
  - ¬ Directory assistance using speech-to-text Google connector

Prompt management

- Upload files: WAV format
- Record from phone: Call or call-back

Interactive Voice Response

- Digit collection
- Correlator data exchange with Alcatel-Lucent OmniTouch Contact Center Standard Edition
- Database read and write
  - ¬ SQL requests
- Test on condition
- Display name customization
- HTTP request
- Email block

Analytics reports

- Web-based interface
  - ¬ Performance pie chart
  - ¬ Statistics per period
  - ¬ Full call log export
- Export capabilities:
  - ¬ Export data to CSV
- Platform or per tenant indicators:
  - ¬ VAA ports usage
  - ¬ Number of calls received
  - ¬ Number of transferred or released calls
  - ¬ Number of calls released by the caller
  - ¬ Number of calls lost due to insufficient license port

Connectivity

- SIP

High availability

- Visual Automated Attendant redundancy
- Support of OmniPCX Enterprise CS:
  - ¬ Geographic redundancy
  - ¬ Passive Communication Server redundancy

Capacity

- Up to 120 ports per server

Support

- SPS

Table 1. Dedicated appliance-type physical server

	Minimum (up to 8 ports)	Recommended (up to 50 ports)	Maximum (up to 120 ports)
Processor	Dual-Core 2.4 GHz	Quad-Core 2.4 GHz	Octo-core 2.4 GHz
Memory	8 GB RAM	16 GB	32 GB
Network	100 Mb/s	1 Gb/s	1 Gb/s
Hard disk	80 GB	80 GB minimum	160 GB

Alcatel·Lucent Enterprise

Overview

When customers engage with your service center, the outcome, convenience and speed of resolution, become **the measurements of your brand** and **company excellence**. There's a lot at stake.

Customer service employees need technology that can handle queries at all stages of the buying cycle, cope with case management, and track issue resolution, to prove return on investment. Whether you are a **small company** or a **multinational**, your customer service solution must be **adapted to your needs, reliable, easy-to-use and to set up**, and most important, **affordable**!

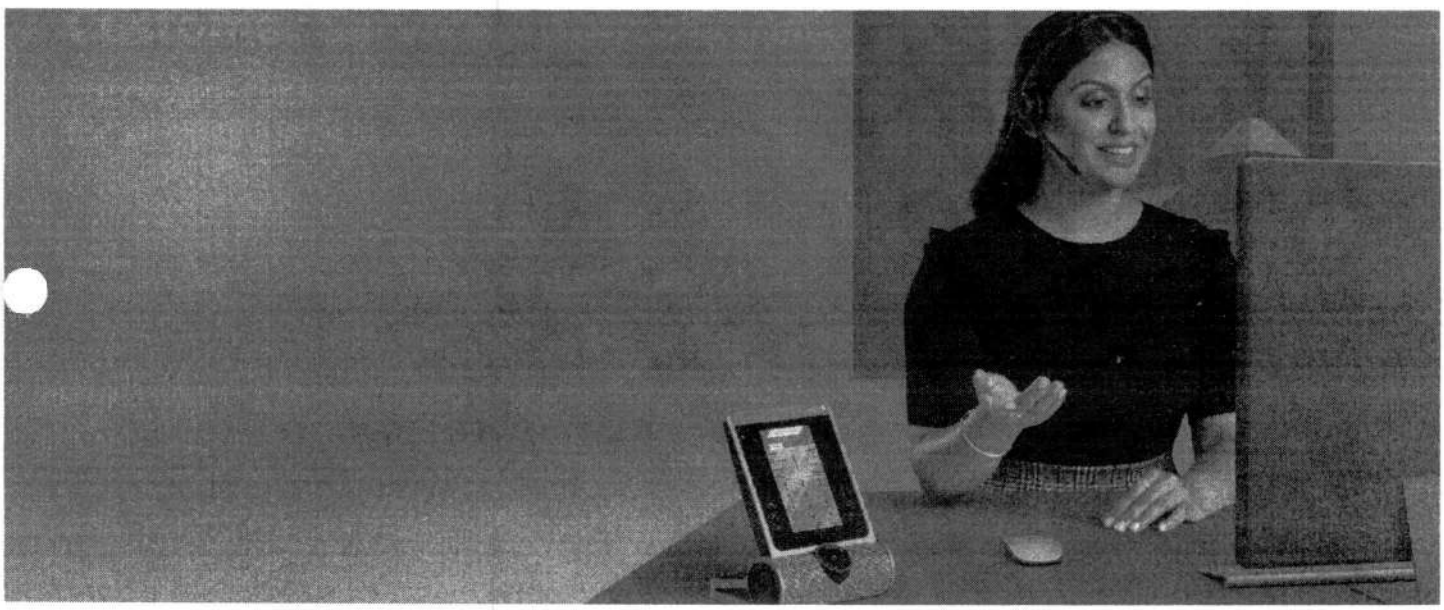
That's where Alcatel-Lucent Enterprise can help you.

Our customer service solutions help you:

- Build a reliable, cost-effective solution that leverage your phone system
- Provide answers to any type of interaction, from **customer welcome** and **automatic call routing**, to advanced **contact center** solutions with connected agents, supervision, and monitoring of activities
- Integrate **omnichannel interactions** (phone, email, SMS, chat, and social media) while maximizing uptime and reliability
- **Connect your existing CRM** solution to leverage your customer database and enrich it with new interactions
- Make your **website** a live portal to your customer community with direct chat (using text, audio, and video) with experts from your customer service team

Here's why businesses choose ALE customer service solutions:

- **A built-in contact center:** Integration between your telephony infrastructure, and the customer service options enable maximum uptime at minimum cost
- **Speed:** Our intuitive systems mean you can onboard new agents fast, minimize training time, and adapt call distribution trees in real-time
- **Simplicity:** A unified global dashboard with multi-channel interactions and transaction data, provided from your CRM tool help simplify your agent's job. You can also easily quantify your ROI based on tight integration with your business applications
- **Scalability:** "Right-size" your customer service operations quickly to meet demand. Our customer service solution models range from modular premises-based solutions to cloud-based, and from CAPEX to pay-per-use



Alcatel-Lucent Enterprise Customer Service Applications

Successful customer relationships for all businesses

Alcatel·Lucent Enterprise

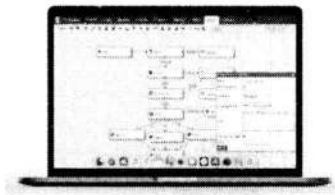
Visual Automated Attendant
Automated 24/7 call routing and greeting

ACCESS TO THE PRODUCT WEB PAGE →

Visual interface to manage rules and prompts

Enterprise calendar management

Multi-tenant delegation



Alcatel-Lucent Visual Automated Attendant qualifies the requests, informs the clients and routes them to the relevant expert or agent.

- **Offer a professional customer welcome:** Expert 24/7 customer response to ensure a professional image and quality
- **Build a recurring business relationship:** Personalized greetings, routing, and news
- **Multi-tenant:** Delegate operations to multiple tenants (different organizations/departments within the company) for better accountability and increased business response
- **Deliver cost-effective operations. Scalable software:** No special IT skills are required to record prompts or manage business hours. Provide a scalable software solution for small to extra-large businesses

24/7 Business response to customers

- *Routing logic based on date and time*
- *Record greetings and prompts from a phone or upload studio quality files*
- *Text-to-speech capabilities (free PICO TTS, IBM Cloud, Google Cloud)*

Adapted and contextual response

- *Prompt messages depending on the context (caller ID, contract number, calendar)*
- *VIP service with special routing*
- *Collect information (IVR) for call qualification and routing*

Cost effective operations

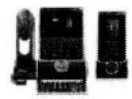
- *Automated welcome adapted for small to large organizations*
- *User-friendly interface for easy personalization without IT assistance*
- *Usage statistics to adapt rules to demand*

ALE offers a wide range of applications for all customer service purposes

- **Automated attendant applications:** Interactive call routing, customer welcome outside of business hours, always-on 24/7
- **Attendant applications**: Personalized, human welcome. From the desk phone or an app on a PC
- **Dispatcher applications**: "Human intelligence" for efficient call dispatch in critical environments
- **Contact center applications**: From agents to supervisors, including call recording and monitoring capabilities
- **Communications applications**: Business communication applications on any device, for all employees including CRM solution users, engaged in customer relationships, using a phone number or company website for live interactions

Customer Welcome Apps

Visual Automated Attendant
Page 4



Attendant app on desk phone
Page 5

Attendant app on PC
Page 6

Dispatcher app
Page 7

Contact Center Apps

OmniTouch Contact Center SE
Page 8

ALE Connect
Page 9

OmniPCX Record Suite
Page 10

Communication App

IP Desktop Softphone
Page 11

Rainbow CRM Connect
Page 12

Rainbow Enterprise
Page 13

30

4059EE Attendant Console PC

Professional welcome with a personal touch

ACCESS TO THE PRODUCT WEB PAGE →

Virtual intuitive user interface on PC

Adapted keyboards with shortcuts for attendant functions

Single or multi-site welcome

Alcatel-Lucent 4059 Extended Edition is an attendant console on PC with an easy-to-use visual interface to provide a personalized customer welcome for medium and large enterprises.

- **Quickly direct calls to the right person the first time:** Receptionist can perform fast directory lookup and see employees presence status directly on the screen
- **Manage a high volume of calls efficiently:** Visual call queuing to handle high traffic
- **Make new or seasonal operators more effective faster:** The solution includes a dedicated ergonomic USB keyboard with attendant functions and the desktop application interface can be customized for any usage
- **Single receptionist for multiple offices:** Centralization and resource sharing to reduce cost

Professional welcome with a personal touch

- *Easy-to-use interface*
- *Waiting queues with indicators*
- *Speed-dial keys*

Efficient call dispatch

- *Busy Lamp Field (BLF) for immediate visibility of respondents' availability*
- *Company directory search engine*
- *Fast-call transfer*

Single or multi-site customer welcome

- *Unified welcome across all locations*
- *Call redirect to predefined number*
- *Mutual help between attendants in different sites*

Attendant application on the desk phone

Professional welcome for branch offices

ACCESS TO THE PRODUCT WEB PAGE →

Professional welcome

Easy to manage and understand

No need for a computer - only a desk phone

The attendant solution on the ALE-300 DeskPhone is intended for enterprises with a medium level of incoming traffic. Functions include management of queued incoming calls with level of urgency identified, and monitoring of internal and external calls.

- **Ergonomic desk phone with visual indications:** Information bar indicating the current date and time, and icons displaying number of waiting call (normal and urgent calls)
- **Extra programming keys:** Expanded capacity with additional key module that plugs into the desk phone. Each key is associated with an electronic icon and label. It is programmed as a resource or supervisory key
- **High audio quality for attendant comfort:** Wired or wireless handset (Bluetooth), and headset jack

Agile attendant desk phone solution

- *Attendant features (including routing management, and call reservation)*
- *Direct visual supervision with key expansion module*
- *Compatible with working from home (VPN embedded phone)*

Effective branch office attendant

- *Adapted for a reduced number of calls and employees*
- *Mutual aid between sites: branch attendant can assist main central attendant*

Cost optimization and ease of use

- *No additional equipment required*
- *Save on installation, configuration and employee training*

31

OmniTouch Contact Center SE

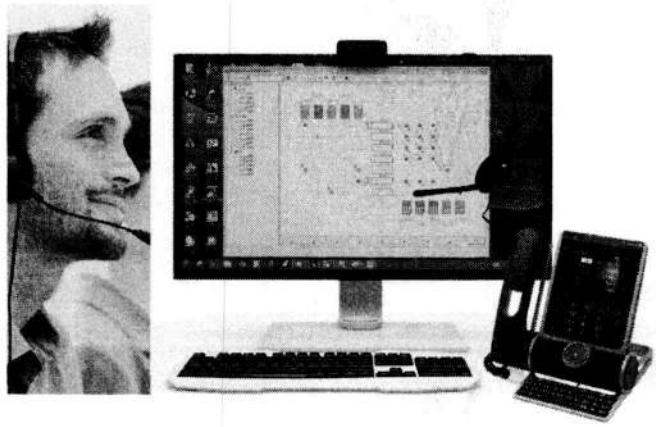
Customer service solution to build successful relationships

ACCESS TO THE PRODUCT WEB PAGE →

All-in-one solution from agent phone and desktop app to supervision

Adapted to remote agent configuration

Extension to multimedia interactions (email, chat, social media)



With Alcatel-Lucent OmniTouch® Contact Center Standard Edition (SE), all organizations – from small businesses and teams looking to organize their customer service, to large companies with contact centers - have access to tools for an efficient and reliable multi-channel customer interaction solution that is easy to implement and integrate with their telephony system.

- **Increased customer satisfaction:** Customers benefit from shorter wait times, as well as the opportunity to speak to a qualified contact
- **Efficiency:** Real-time supervision applications and detailed reports optimize processes in the short and long-term
- **Cost-saving:** Permanent access to contact center features is available from the agent's phone without complex IT integration
- **Reliability:** High availability of the communication server enables better call distribution and maximum service continuity

Efficient call distribution

- *Patented visual tool to manage configuration, design routing and check call flows*
- *Routing time schedule*
- *Skill-based distribution*
- *Group selection options*

Empowered agents and supervisors

- *Free seating agent position, desk phone or softphone, open to remote agent configuration*
- *Supervisor with discrete call listening and monitoring*
- *Desktop application for agent and supervisor*

Built-in flexibility and reliability

- *Integrated with OmniPCX® Enterprise on-premises, or in the cloud*
- *Add-on module (Soft Panel Manager) to display statistics and business data on wallboard, screen and mobile devices*
- *Add-on module for omnichannel with email, chat, social media and CRM applications integration*

Dispatch Console

"Human Intelligence" solution for call processing

ACCESS TO THE PRODUCT WEB PAGE →

Dispatch high volume of calls stress free

Dispatcher app available on desktop or touchscreen

Integration with 3rd party control center app

Alcatel-Lucent Enterprise Dispatch Console enables the presentation and selection of calls according to business processes and priority rules, based on operator decisions. It is ideally suited for control centers (such as railway, airport, energy supplier, and public emergency), as well as environments where call qualification and call selection are needed.

- **Manage high volume of calls:** Presentation and dispatch by the operator based on priority rules
- **Visual and intuitive interface:** Operators can route calls, manage queue(s), and set up conferences
- **Web interface:** Accessible from the desktop PC, touchscreen workstation, or integrated with a 3rd party control center application (such as SCADA supervision platform)

Coordinate operations and share information

- *Speed dial/dial pad to quickly distribute calls*
- *Multiple routing options: transfer, park or put in a queue*
- *3-party conference, and conference up to 60 participants (optional)*

Full control and integration

- *Administration module: Manage the operator console display, configuration with templates, statistics generation*
- *Integration with the company LDAP directory*
- *Integration within a 3rd party control center application (such as SCADA supervision platform)*

Secure and reliable communications

- *Supervision by one or more operators simultaneously*
- *Call history for operations tracking and callback on missed calls*
- *High availability with server duplication and Alcatel-Lucent OmniPCX® Enterprise geo-redundancy*

32

OmniPCX RECORD Suite

When everything must be on the record

ACCESS TO THE PRODUCT WEB PAGE →

Base package offers voice recording for inbound and outbound calls

Add screen capture to the record application

Offers quality reporting and evaluation analysis

Alcatel-Lucent OmniPCX® RECORD Suite provides businesses with a reliable application to record and supervise calls that support quality assurance, accelerate customer issue resolution, boost loyalty and streamline

- **Efficient risk management:** In the event of a dispute, a recording of the interaction can provide verification of the exchange between customers and agents
- **Regulatory compliance and data protection:** The solution meets the legal requirements for payment by phone (PCI-DSS), and interactions with financial institutions (MiFID II). The solution also provides strict security management policies for high protection of customer data
- **Improved quality of service:** The customizable quality monitor application helps managers identify areas requiring improvement. Coaching tools and tutorials help improve employee and agent performance
- **Easy and cost-effective implementation:** Seamless integration into existing or newly installed OmniPCX Enterprise environments. The user-friendly web-based interface offers fast access to all features (including consultation of call records from other recorders)

Enterprise solution for real-time call recording

- *On-demand, retro-active, random and total recording of all conversations*
- *Embedded playback*
- *Multiple criteria search*
- *Multi-channel call recording: Phone, trunk, SIPREC*

Capture screen to support audio recording

- *Screen capture web interface*
- *Complete user desktop activity capture*
- *Extended desktop capture*

Quality monitor

- *Customizable score cards*
- *Reporting on individual or group achievements*
- *Dashboard providing an overview of performance evolution*
- *Coaching sessions based on scorecards, with annotations and learning attachments*

ALE Connect

Complete solution for omnichannel contact center management

ACCESS TO THE PRODUCT WEB PAGE →

Omnichannel interactions (phone, email, chat, social media)

Automation of repetitive tasks with intelligent assistance

Cloud based services work from anywhere

Alcatel-Lucent Enterprise Connect (ALE Connect) enables customer services of all sizes, handling omnichannel interactions with the quality and efficiency expected by today's customers, citizens, and consumers.

- **Efficiency:** Optimised distribution of the customer requests, whatever the channel, based on competences and availability of the agents
- **Global view:** Centralised customer data to deliver a 360° view of the customer context to the agent, including contact information (from built-in database or extracted from external CRM/ERP application) and history of the previous interactions whatever the channel used
- **High quality interactions:** A unique desktop interface for the agent to manage all the available channels. Highlight contact information of the online customer. Intuitive cross-channel during a conversation, to improve efficiency and first contact resolution
- **Control:** Agent and supervisor can access graphical dashboards for all digital channels and benefit from complete visibility on the real-time performance. Detailed reports to optimise processes over the long term

Connect your customers their way

- *Connect using voice, email, chat live through the company web site, Facebook Messenger, Twitter*
- *Manage voice calls using ALE Contact Center from within the Agent Desktop App*
- *Empower agents with a unified web-based application on the desktop*

Improve first contact resolution

- *Display customer information using built-in database or CRM*
- *See history of past interactions across all channels in a single window*
- *Search in the built-in knowledge base with standard responses, and the intelligent assistance to suggest best answers depending on the context*

Adapt smoothly using hybrid cloud

- *Leverage ALE phone system, licenses, phone sets and softphones. Keep voice Contact Center routing rules adapted to your needs*
- *Plug-and-Play: automated cloud provisioning of agents/ processing groups*
- *Adapt costs to business: nothing to install to scale, flexible subscriptions*

Rainbow CRM Connect

ACCESS TO THE PRODUCT WEB PAGE →

Empower your favorite Customer Relationship Management (CRM) application with telephony and collaboration

Customer form popup on incoming call

Click-to-call from the CRM app

Market leading CRM integration

Provide customers with a quick and personalized response with Alcatel-Lucent

- **Reduce wait time for your customers during peak activity:** the service is available, for as long as you want and can be quickly implemented from the cloud
- **Provide a personalized customer service:** Employees have automatic access to the customer's form when customers call your company
- **Call your customers back with confidence:** Your customers' phone numbers are automatically captured by Rainbow and added to the CRM. No typing errors are possible. One click calling makes it easy to get in touch
- **Provide your customers with the information they want on the very first call:** Employees can help each other by exchanging files, instant messaging or making phone calls from within the CRM application

Easy-to-deploy CRM integration

- *Salesforce, Microsoft Dynamics, ServiceNow, Zoho CRM*
- *Just download an add-in*
- *Seamless user experience within the CRM desktop application*

Customer information

- *Automated recording of the customer's phone number*
- *Form pop-up on incoming call*

Click-to-call

- *Call on PC or from a business phone*
- *Click on numbers in CRM form to call*
- *Call or chat with colleagues*

IP Desktop Softphone

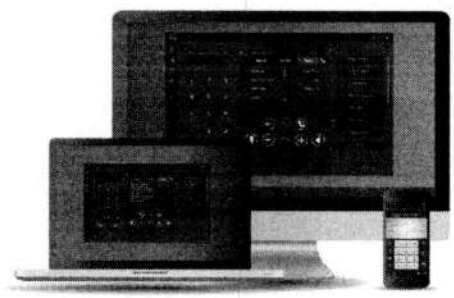
ACCESS TO THE PRODUCT WEB PAGE →

Software phone for PC, Mac, Tablets and Smartphones

Same interface and functionality as the ALE DeskPhone

Agent features

Easy remote installation



User-friendly and easy to install, the Alcatel-Lucent IP Desktop Softphone offers all the ALE DeskPhone features on PC, Mac, or Android. It turns your computer or mobile into a high-end enterprise grade VoIP phone at the price of a regular phone. Cost-effective: No additional server required. As easy to manage as a desk phone for all employees, including contact center agents.

- **Device of choice anywhere:** Employees who have no physical desk phones are always reachable on computer, tablet or smartphone
- **Employee efficiency:** All telephony services are available, including contact center agent features
- **Easy adoption:** No additional user training required when users are familiar with the desk phone

Complete business telephony

- *Display and usages similar to ALE DeskPhones*
- *Multi-line and call supervision*
- *Use Alcatel-Lucent OmniPCX® Enterprise or OXO Connect telephone features*

Contact center agent features [1]

- *Login/Logoff, wrap-up*
- *Supervisor functionality*
- *Call distribution and routing rules with a remote agent*

[1] OmniTouch Contact Center SE

Any device, anywhere availability

- *Computer (PC, Mac OS), tablet or smartphone (Android), compatibility VDI*
- *Leverage the company VPN for off-site/remote worker usages*
- *No mix between private and professional life (smartphone)*

34

More Information

Check out our e-catalog desk phones
Check out our e-catalog mobile phones

Alcatel·Lucent Enterprise

Rainbow Enterprise

ACCESS TO THE PRODUCT WEB PAGE →

Universal communication app connected to the phone and the company web site to engage customers

Receive your business calls on any device

Engage audio and video with visitors from web

Collaborate with the team for fast customer problem resolution

Office and mobile employees work together with Alcatel-Lucent Rainbow Enterprise to

- **Manage customers' calls with confidence, even when out of the office**: Call from your mobile or computer using your business line. Look for a quick answer or need to transfer an important call? See who's available and manage everything from your mobile
- **Engage with customers connected to the company website looking for support through live chat or an audio & video call:** Provide the best of connected website for visitors, and enable any of your employees to get involved in customer support
- **Collaborate with people in groups and teams:** Use chat, audio and video conferencing, and exchange files securely. Rainbow is certified secure and locally hosted. Your company's and your customers' data are safe!

Business calls on mobile and more

- *Route calls on mobile, laptop, and desktop phone from an app*
- *See if contact is online, on the phone, or in a meeting*

Engagement multi-channels

- *Chat, audio and video call*
- *Conferencing with 120+ participants*
- *Integration within the company website to engage live with visitors*

Secure team collaboration

- *Chat groups with up to 300 participants*
- *Text messaging, 20 Gb file sharing*
- *ISO 27001 security certification, local hosting, strict confidentiality policy*

35

Alcatel·Lucent
Enterprise

Alcatel-Lucent OmniVista 8770 Network Management System

The Alcatel-Lucent OmniVista® 8770 Network Management System (NMS) is an all-in-one graphical management application that offers a unified view of your ALE communication network. It's simple to use, configure and operate from a single interface. Moreover, it automates operations by synchronizing with Microsoft Active Directory.

Communications are critical for your business. The OmniVista 8770 NMS helps you stay in control and have visibility on SLAs. It follows the FCAPS model of network management which includes instant alarm notifications, accounting reports and performance monitoring, all from a single comprehensive application suite.

Features	Benefits
Light web client including Unified User Management, OXE network configuration and Performance dashboard.	Web user friendly, no footprint on the administrators' PC.
Unified user management: Manage frequent users Move/Add/Change/Deletion (MACD), multi domains and right delegation. Get custom views. Manage one or several communication servers.	Efficiency: Spend less time on basic user management and delegate user provisioning. Focus on high-value tasks instead.
Microsoft Active Directory (MSAD) synchronization: The OmniPCX Enterprise and MSAD users are automatically synchronized.	Improve user experience and save time: Automate processes and prevent directory inconsistencies.
OmniPCX Enterprise network real-time configuration	Save time by a quick access to the full configuration of the OmniPCX Enterprise network via a single client
Automated remote system back-up and upgrade	Avoid configuration data loss and always get the latest release.
Alarm monitoring: Instant notification on communication system failures or quality alerts.	Network availability: Immediately notify the appropriate people when communication systems issue critical alarms.
Topology graphical views: See communication server network performance on a map	Durability: Pre-empt potential network issues, be proactive on maintenance.
Accounting reports including threshold monitoring and cost tracking. Automatic report generation and notification.	Cost control: Manage multi-carrier and multi-currency billing. Reduce telecommunications costs by tracking abuses. Provide internal re-invoicing.
Communications and voice-over-IP performance monitoring: including users, trunks, radio base stations, attendants etc. Performance dashboards: OXE health, quality, activity, trunks and IP domains.	Control: Analyze usage and quality trends by tracking metrics. Ensure the communication infrastructure size corresponds to your business.
Manage My Phone: For OXE users to manage their phone set from a web page.	Simplicity: user friendly web interface to personalize the desk phone.

Datasheet
Alcatel-Lucent OmniVista 8770 Network Management System

Technical specifications

Unified User Management[1]

- Quick user provisioning with profiles
- SIP devices deployment and user association
- Mass provisioning (including Rainbow users)
- User configuration
- MS Active Directory synchronization and user provisioning
- Multi domains and customized views

Company Directory[1]

- Access to corporate directory information through a web browser
- Click-to-call
- Automatic updates through internal and external directories
- Access through standard LDAP V3 clients

System configuration

- Alcatel-Lucent OmniPCX Enterprise Communication Server (CS)
- Alcatel-Lucent OpenTouch Multimedia Services (MS) and OpenTouch Message Center (MC)
- Alcatel-Lucent OXO Connect and OmniPCX Office RCE
- Graphical view[1,2] of Alcatel-Lucent Smart DeskPhone, Premium DeskPhone, DeskPhone, DeskPhone 8 Series, DeskPhone 9 Series, ALE Enterprise and Essential DeskPhones, ALE-2

Topology and alarms monitoring

- Notifications of urgent situations
- Topology maps

Accounting

- Multi-carrier and multi-currency accounting
- Consolidated view of telecommunications expenses
- Delivered with a set of predefined reports
- Possibility to create personalized reports

Performance monitoring

- Notification of threshold crossing
- Attendants, trunks[1,2], base stations and VoIP communications[2] performances monitoring
- OmniPCX Enterprise web performance dashboard

APIs

- Proxy SNMP for alarms
- Ticket collector for VoIP performance and accounting
- OpenAPI for users provisioning[1]

Managed Communication Services Edition

- Automated emailing to lists of customers according to their preferences
- Consolidated alarms monitoring
- Backups, upgrades
- User MAC (Moves, Adds and Changes)
- Performance and accounting
- Multi domains[1]
- Asset management

Start pack

- Unified management
- Accounting
- Alarms monitoring

Full pack

- Start pack features
- Performance monitoring
- Web company directory

Supported systems

- OmniPCX Enterprise CS from R6.0 and R100 Purple
- OmniPCX Office RCE from R5.1
- OXO Connect from R2.0
- OpenTouch MS and OpenTouch MC from R1.3

Hardware requirements and OS support for server stations

- Medium range (up to 5000 users)
  - ¬ Dual core 2 GHz or higher
  - ¬ RAM: 6 GB RAM
  - ¬ Hard Disk: 120 GB
  - ¬ Windows 8.1 Pro
  - ¬ Windows 10 Pro or Enterprise
- High range (more than 5000 users)
  - ¬ Quad core 2 GHz or higher
  - ¬ RAM: 8 GB
  - ¬ Hard Disk: 120 GB
  - ¬ Raid 5, 512 MB cache memory min.
  - ¬ Windows Server 2012 R2 Datacenter and Standard Edition
  - ¬ Windows Server 2016 Datacenter and Enterprise
  - ¬ Windows Server 2019 Datacenter and Standard Edition

Virtualization

- OmniVista 8770 NMS server
  - ¬ VMware ESXi
  - ¬ Microsoft Hyper-V
- OmniVista 8770 NMS client
  - ¬ Citrix XenApp server

Provisioning level

- Users managed on one server with Full Pack: 50,000 users
- Number of managed communication servers: 300

Security

- Active and passive redundancy
- Public Key Infrastructure (PKI)
- Role-based and domain management

Supported browsers for web Directory access

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Microsoft Internet Explorer

Supported browsers for users administration access (web client)

- Google Chrome
- Mozilla Firefox

Languages

- English, French, German, Spanish, Portuguese, Italian, Polish, Slovakian, Chinese (SCH), Czech, Russian, Hungarian, Korean, Croatian, Traditional Chinese

1 Not available for OXO Connect, OmniPCX Office RCE
2 Not available for OpenTouch MS and MC

37

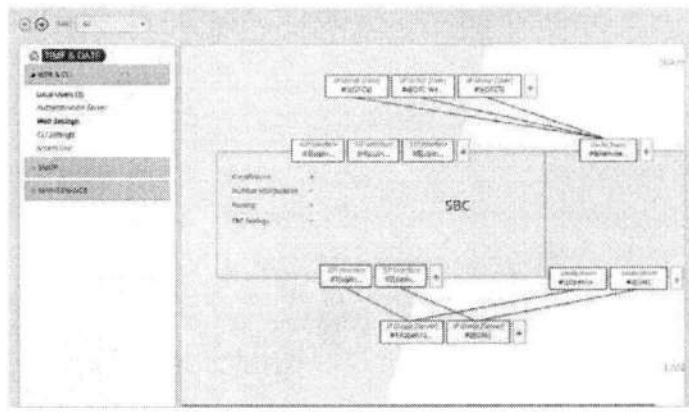
Alcatel·Lucent Enterprise

Alcatel·Lucent
Enterprise

Alcatel-Lucent OpenTouch Session Border Controller

Protect SIP trunks and enterprise communications with a highly secure SIP perimeter defense solution

The Alcatel-Lucent OpenTouch® Session Border Controller (OpenTouch SBC) addresses the communication security needs of mid-sized and large organizations by protecting them from malicious VoIP attacks, SIP denial of service, and fraud and eavesdropping.



As a highly secure software solution for perimeter defense, OpenTouch SBC acts as the demarcation point between the enterprise and SIP trunking providers. OpenTouch SBC also protects mobile workers and secures their SIP audio and video communications over the internet.

Features	Benefits
Enterprise perimeter defense against SIP denial of service, fraud and eavesdropping	Security: Reinforces firewalls with dedicated protection against SIP-based attacks
Secure and scalable SIP/media connectivity, audio transcoding an network address translation (NAT) traversal for audio and video communications	Cost-saving: Ensures cost-effective, secure conversations over the internet and with SIP service providers
Web-based management with built-in configuration templates: settings and protocol adaptations for certified SIP trunking providers can be configured in a few clicks	Cost-effective interoperability: Offers protocol adaptations for many SIP trunking providers
Redundant servers with SIP and media session preservation	Business continuity: Offers always-on, off-net and mobile communications
VMware vSphere Hypervisor and Microsoft Hyper-V support	Agile operations: Leverages virtualization infrastructure and skills

38

Technical specifications

Solutions

- OEM AudioCodes Mediant Virtual Edition
- SIP trunking security solution for:
  - ¬ Alcatel-Lucent OmniPCX® Enterprise Communication Server R12.3 and above
  - SIP remote worker security solution for:
  - ¬ Alcatel-Lucent OmniPCX Enterprise Communication Server R12.3 and above
  - ¬ Alcatel-Lucent OpenTouch® Multimedia Services R2.4
  - ¬ Alcatel-Lucent OpenTouch® Conversation software clients
  - ¬ WebRTC access to OpenTouch MS conferences
  - ¬ ALE SoftPhone R100 and above
  - ¬ HTTPS Reverse Proxy access to OpenTouch MS or OXE SIP Device Management
- Private SIP trunking with Microsoft Teams Direct Routing:
  - ¬ Alcatel-Lucent OmniPCX Enterprise Communication Server R12.4 and above
- SIPREC trunk recording solution for:
  - ¬ OmniPCX Record R2.4 and above

Security

- Miercom certified
- Distributed denial of service (DDOS) prevention: L3/L4 and SIP
- SIP stateful inspection: Prevents DDOS attacks based on fraudulent SIP messages
- SIP topology hiding: SIP headers that disclose internal IP topology are removed or modified
- Secure SIP over Transport Layer Security (TLS) (SIPS): Encryption and authentication of SIP messages, SIP over WSS for WebRTC
- Secure Real-time Transport Protocol (SRTP): Encryption of audio and video streams SDES and DTLS crypto key negotiation (AES 128/256)
- Dynamic audio and video port firewall pinholing
- Signature based SIP Intrusion Detection System (IDS) and dynamic blacklisting
- SIP authentication (http digest) of clients and gateways
- Enhanced media latching
- Integrated NGINX Light Reverse Proxy
- Complements NGINX+ standalone for low end
- LDAP authentication

Management

- Manageable by AudioCodes One Voice Operation Center (OVOC) platform
- Secured web-based management
- Zero user management: Provisioning of directory number, SIP user information and security credentials are delegated to the communication server
- Simple Network Management Protocol (SNMP)
- Built-in SBC wizard application for SIP trunking and remote worker scenarios
- Multi-Tenancy for OTEC (SBC only, no Reverse Proxy)

Business continuity

- Alternative routing and load balancing:
  - ¬ Detects lost connectivity to the communication server and to the SIP provider's proxy servers, and routes to alternative servers
  - ¬ Supports OmniPCX Enterprise geographic redundancy
  - ¬ Supports load balancing across a pool of SIP provider proxy servers
  - ¬ Least-cost routing (based on date, time and cost)
- High-availability option: Active/standby two-server redundancy
  - ¬ Active SIP and media sessions are preserved
  - ¬ Virtual IP
- Software upgrade without interruption

Interoperability and protocols

- SIP B2BUA: SIP transparency
- SIP WebRTC gateway
- RFCs supported: RFC 2327, RFC 2617, RFC 2782, RFC 2833, RFC 2976, RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3265, RFC 3311, RFC 3323, RFC 3325, RFC 3362, RFC 3420, RFC 3455, RFC 3489, RFC 3515, RFC 3550, RFC 3581, RFC 3611, RFC 3665, RFC 3666, RFC 3711, RFC 3725, RFC 3824, RFC 3842, RFC 3891, RFC 3892, RFC 3903, RFC 3960, RFC 3966, RFC 4028, RFC 4117, RFC 4168, RFC 4235, RFC 4244, RFC 4320, RFC 4321, RFC 4475, RFC 4566, RFC 4568, RFC 4582, RFC 4730, RFC 4733, RFC 4960, RFC 4961, RFC 4975, RFC 5022, RFC 5079, RFC 5124, RFC 5245, RFC 5389, RFC 5628, RFC 5761, RFC 5763, RFC 5764, RFC 5806, RFC 5853, RFC 6035, RFC 6135, RFC 6140, RFC 6188, RFC 6337, RFC 6341, RFC 6442, RFC 7245, RFC 7261, RFC 7865, RFC 7866, RFC 8068
- Transport mediation: SIP over UDP to SIP over TCP, or SIP over TLS, or SIP over WSS
- SIP call-flow mediation
- Real-time audio mediation option: RTP to SRTP encryption
- Extensive SIP profile configuration with third-party SIP Providers
- Extensive SIP signaling interworking: 3xx forwarding Termination, Refer to Reinvite, Diversion Header to History Info, Prack and Update termination
- Programmable header manipulation: Ability to add, modify and delete headers
- Programmable SDP manipulation: Codec list rewriting
- Programmable routing methods: Request URL, source/destination IP address, fully qualified domain name, ENUM, Lightweight Directory Access Protocol
- Uniform resource identifier (URI) and number manipulations:
  - ¬ URI user and host name manipulations
  - ¬ Ingress and egress digit manipulations
- NAT traversal: Local and far end NAT traversal for support of remote workers
- Audio and video codec filtering
- Audio software transcoding:
  - ¬ inband DTMF
  - ¬ G711A/G711Mu law
  - ¬ Opus, Silk

Media quality and reporting

- Packet marking: 802.1p/Q VLAN tagging, DiffServ, TOS
- Media Anchoring or Direct Media
- Transparent media: Low latency, unprocessed payload transfer
- Voice quality measurement: Voice quality call detail record generation
- RTP Control Protocol-XR support with SIP Publish
- Call Admission Control on media bandwidth, including audio and video
- Allocation of a minimal number of sessions to dedicated SIP interfaces
- Alternative routing based on quality and bandwidth

39

Capacity and VM prerequisites (VMWare)	Virtual Edition high end	Virtual Edition medium	Virtual Edition low end
Max. SIP endpoints/TLS sessions	6000/6000	6000/6000	1000/1000
Max. SIP sessions	4000	2600/1900/1600	250
Max. RTP/SRTP (*0/1/n vCPUs transcoding)	4000	*2600/1900/1600	250
vCPUs/GB RAM/GB HDD/ HyperThreading (HT)	4vCPUs/16 GB RAM/ 10 GB HDD/HT	1vCPU/8 GB RAM/ 10GB HDD/HT	1vCPU/2 GB RAM/ 10 GB HDD/HT
Transcoding	by adding 4 or 12 vCPUs	by adding 1 or 3 vCPUs	N/A

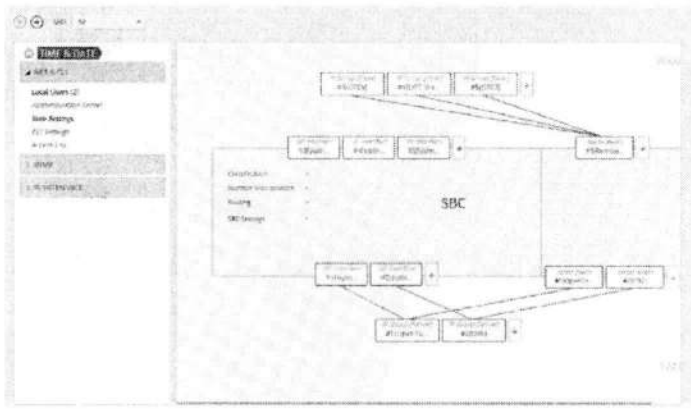
Alcatel·Lucent Enterprise

Alcatel·Lucent
Enterprise

Alcatel-Lucent OpenTouch Session Border Controller

Protect SIP trunks and enterprise communications with a highly secure SIP perimeter defense solution

The Alcatel-Lucent OpenTouch® Session Border Controller (OpenTouch SBC) addresses the communication security needs of mid-sized and large organizations by protecting them from malicious VoIP attacks, SIP denial of service, and fraud and eavesdropping.



As a highly secure software solution for perimeter defense, OpenTouch SBC acts as the demarcation point between the enterprise and SIP trunking providers. OpenTouch SBC also protects mobile workers and secures their SIP audio and video communications over the internet.

Features	Benefits
Enterprise perimeter defense against SIP denial of service, fraud and eavesdropping	Security: Reinforces firewalls with dedicated protection against SIP-based attacks
Secure and scalable SIP/media connectivity, audio transcoding an network address translation (NAT) traversal for audio and video communications	Cost-saving: Ensures cost-effective, secure conversations over the internet and with SIP service providers
Web-based management with built-in configuration templates: settings and protocol adaptations for certified SIP trunking providers can be configured in a few clicks	Cost-effective interoperability: Offers protocol adaptations for many SIP trunking providers
Redundant servers with SIP and media session preservation	Business continuity: Offers always-on, off-net and mobile communications
VMware vSphere Hypervisor and Microsoft Hyper-V support	Agile operations: Leverages virtualization infrastructure and skills

Technical specifications

Solutions

- OEM AudioCodes Mediant Virtual Edition
- SIP trunking security solution for:
  - ¬ Alcatel-Lucent OmniPCX® Enterprise Communication Server R12.3 and above
  - SIP remote worker security solution for:
  - ¬ Alcatel-Lucent OmniPCX Enterprise Communication Server R12.3 and above
  - ¬ Alcatel-Lucent OpenTouch® Multimedia Services R2.4
  - ¬ Alcatel-Lucent OpenTouch® Conversation software clients
  - ¬ WebRTC access to OpenTouch MS conferences
  - ¬ ALE SoftPhone R100 and above
  - ¬ HTTPS Reverse Proxy access to OpenTouch MS or OXE SIP Device Management
- Private SIP trunking with Microsoft Teams Direct Routing:
  - ¬ Alcatel-Lucent OmniPCX Enterprise Communication Server R12.4 and above
- SIPREC trunk recording solution for:
  - ¬ OmniPCX Record R2.4 and above

Security

- Miercom certified
- Distributed denial of service (DDOS) prevention: L3/L4 and SIP
- SIP stateful inspection: Prevents DDOS attacks based on fraudulent SIP messages
- SIP topology hiding: SIP headers that disclose internal IP topology are removed or modified
- Secure SIP over Transport Layer Security (TLS) (SIPS): Encryption and authentication of SIP messages, SIP over WSS for WebRTC
- Secure Real-time Transport Protocol (SRTP): Encryption of audio and video streams SDES and DTLS crypto key negotiation (AES 128/256)
- Dynamic audio and video port firewall pinholing
- Signature based SIP Intrusion Detection System (IDS) and dynamic blacklisting
- SIP authentication (http digest) of clients and gateways
- Enhanced media latching
- Integrated NGINX Light Reverse Proxy
- Complements NGINX+ standalone for low end
- LDAP authentication

Management

- Manageable by AudioCodes One Voice Operation Center (OVOC) platform
- Secured web-based management
- Zero user management: Provisioning of directory number, SIP user information and security credentials are delegated to the communication server
- Simple Network Management Protocol (SNMP)
- Built-in SBC wizard application for SIP trunking and remote worker scenarios
- Multi-Tenancy for OTEC (SBC only, no Reverse Proxy)

Business continuity

- Alternative routing and load balancing:
  - ¬ Detects lost connectivity to the communication server and to the SIP provider's proxy servers, and routes to alternative servers
  - ¬ Supports OmniPCX Enterprise geographic redundancy
  - ¬ Supports load balancing across a pool of SIP provider proxy servers
  - ¬ Least-cost routing (based on date, time and cost)
- High-availability option: Active/standby two-server redundancy
  - ¬ Active SIP and media sessions are preserved
  - ¬ Virtual IP
- Software upgrade without interruption

Interoperability and protocols

- SIP B2BUA: SIP transparency
- SIP WebRTC gateway
- RFCs supported: RFC 2327, RFC 2617, RFC 2782, RFC 2833, RFC 2976, RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3265, RFC 3311, RFC 3323, RFC 3325, RFC 3362, RFC 3420, RFC 3455, RFC 3489, RFC 3515, RFC 3550, RFC 3581, RFC 3611, RFC 3665, RFC 3666, RFC 3711, RFC 3725, RFC 3824, RFC 3842, RFC 3891, RFC 3892, RFC 3903, RFC 3960, RFC 3966, RFC 4028, RFC 4117, RFC 4168, RFC 4235, RFC 4244, RFC 4320, RFC 4321, RFC 4475, RFC 4566, RFC 4568, RFC 4582, RFC 4730, RFC 4733, RFC 4960, RFC 4961, RFC 4975, RFC 5022, RFC 5079, RFC 5124, RFC 5245, RFC 5389, RFC 5628, RFC 5761, RFC 5763, RFC 5764, RFC 5806, RFC 5853, RFC 6035, RFC 6135, RFC 6140, RFC 6188, RFC 6337, RFC 6341, RFC 6442, RFC 7245, RFC 7261, RFC 7865, RFC 7866, RFC 8068
- Transport mediation: SIP over UDP to SIP over TCP, or SIP over TLS, or SIP over WSS
- SIP call-flow mediation
- Real-time audio mediation option: RTP to SRTP encryption
- Extensive SIP profile configuration with third-party SIP Providers
- Extensive SIP signaling interworking: 3xx forwarding Termination, Refer to Reinvite, Diversion Header to History Info, Prack and Update termination
- Programmable header manipulation: Ability to add, modify and delete headers
- Programmable SDP manipulation: Codec list rewriting
- Programmable routing methods: Request URL, source/destination IP address, fully qualified domain name, ENUM, Lightweight Directory Access Protocol
- Uniform resource identifier (URI) and number manipulations:
  - ¬ URI user and host name manipulations
  - ¬ Ingress and egress digit manipulations
- NAT traversal: Local and far end NAT traversal for support of remote workers
- Audio and video codec filtering
- Audio software transcoding:
  - ¬ inband DTMF
  - ¬ G711A/G711Mu law
  - ¬ Opus, Silk

Media quality and reporting

- Packet marking: 802.1p/Q VLAN tagging, DiffServ, TOS
- Media Anchoring or Direct Media
- Transparent media: Low latency, unprocessed payload transfer
- Voice quality measurement: Voice quality call detail record generation
- RTP Control Protocol-XR support with SIP Publish
- Call Admission Control on media bandwidth, including audio and video
- Allocation of a minimal number of sessions to dedicated SIP interfaces
- Alternative routing based on quality and bandwidth

42

Capacity and VM prerequisites (VMWare)	Virtual Edition high end	Virtual Edition medium	Virtual Edition low end
Max. SIP endpoints/TLS sessions	6000/6000	6000/6000	1000/1000
Max. SIP sessions	4000	2600/1900/1600	250
Max. RTP/SRTP (*0/1/n vCPUs transcoding)	4000	*2600/1900/1600	250
vCPUs/GB RAM/GB HDD/ HyperThreading (HT)	4vCPUs/16 GB RAM/ 10 GB HDD/HT	1vCPU/8 GB RAM/ 10GB HDD/HT	1vCPU/2 GB RAM/ 10 GB HDD/HT
Transcoding	by adding 4 or 12 vCPUs	by adding 1 or 3 vCPUs	N/A

Alcatel·Lucent Enterprise

Alcatel·Lucent
Enterprise

Alcatel-Lucent OpenTouch™ Session Border Controller – R7.4

Release Note

8AL90062USAHed01
09/2021

Table of Contents

List of Tables

45

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://myportal.al-enterprise.com

This document is subject to change without notice.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Related Documentation

Document Title - Reference	
Alcatel-Lucent OpenTouch™ Session Border Controller – R7.4 Configuration Guide	8AL90065USAled01
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4 SNMP Reference Guide	8AL90067USAFed01
Alcatel-Lucent OpenTouch™ Session Border Controller – R7.4 Release Note	8AL90062USAHed01
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4 SIP Message Manipulation Reference Guide	8AL90543USAFed01
Alcatel-Lucent OpenTouch™ Session Border Controller – R7.4 Performance monitoring parameters and alarms	8AL90557USABed01
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4 Recommended Security Guidelines Configuration Note	8AL90063USAFed01
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4 Virtual Edition REST API for Devices	8AL90078USAAed01
Alcatel-Lucent OpenTouch™ Session Border Controller - R7.4 Version 7.2 to 7.4 Upgrade Procedure Configuration note	8AL90079USAAed01

1 Introduction

This document describes the Latest Release (LR) versions for Release 7.4 for AudioCodes' session border controllers (SBC) and media gateways.

Note:

- Some of the features mentioned in this document are available only if the relevant software License Key has been purchased from AudioCodes and is installed on the device. For a list of available License Keys that can be purchased, please contact your AudioCodes sales representative.
- Open source software may have been added and/or amended. For further information, visit AudioCodes website at https://www.audiocodes.com/services-support/open-source or contact your AudioCodes sales representative.
- Updates to this document may be made due to significant information discovered after the release or too late in the release cycle to be otherwise included in this release documentation. You can check for an updated version on AudioCodes website at https://www.audiocodes.com/library/technical-documents.

1.1 Software Revision Record

The following table lists the LR versions for Release 7.4.

Note: The latest software versions can be downloaded from AudioCodes' Services Portal (registered Customers only) at https://services.audiocodes.com.

Table 1-1: Software Revision Record of LR Versions

Software Version	Released Date
7.40A.100.233 (7.4.100-2)	1 September 2021
7.40A.100.114 (7.4.100-1)	1 July 2021
7.40A.100.021 (7.4.100-01)	19 May 2021
7.40A.100.011 (7.4.100)	3 May 2021
7.40A.005.613 (7.4_R2-4)	1 August 2021
7.40A.005.509 (7.4_R2-1)	6 April 2021
7.40A.005.314 (7.4_R2)	16 February 2021
7.40A.002.007	29 October 2020

1.2 Supported Products

The following table lists the SBC and Media Gateway products supported in this release.

Note:

- Product support and hardware configurations may change without notice. Currently available hardware configurations are listed in AudioCodes Price Book. For further enquiries, please contact your AudioCodes sales representative.
- Figures shown in the tables in this section are maximum values per interface. For available hardware configurations including combinations of supported interfaces, contact your AudioCodes sales representative.

Table 1-2: SBC and Media Gateway Products Supported in Release 7.4

Product	Telephony Interfaces			Ethernet Interfaces	USB	OSN
	FXS/FXO	BRI	E1/T1			
Mediant 500 Gateway & E-SBC	-	-	1/1	4 GE	2	-
Mediant 500L Gateway & E-SBC	4/4	4	-	4 GE	1	-
Mediant 800B Gateway & E-SBC	12/12	8	2	4 GE / 8 FE	2	√
Mediant 800C Gateway & E-SBC	12/12	8	4	4 GE / 8 FE	2	√
Mediant 1000B Gateway & E-SBC	24/24	20	6/8	7 GE	-	√
MP-1288 Gateways & E-SBC	288/0	-	-	2 GE	1	-
Mediant 2600 E-SBC	-	-	-	8 GE	-	-
Mediant 4000 SBC	-	-	-	8 GE	-	-
Mediant 4000B SBC	-	-	-	8 GE	-	√
Mediant 9030 SBC	-	-	-	12 GE	-	-
Mediant 9080 SBC	-	-	-	12 GE	-	-
Mediant SE SBC	-	-	-	12 GE	-	-
Mediant VE SBC	-	-	-	12 GE	-	-
Mediant CE SBC	-	-	-	12 GE	-	-

1.3 Terms Representing Product Groups

Throughout this document, the following terms are used to refer to groups of AudioCodes products for feature applicability. Where applicability is specific to a product, the name of the product is used.

Table 1-3: Terms Representing Product Groups

Term	Product
Analog	Products with analog interfaces (FXS or FXO): • MP-1288 • Mediant 500L Gateway & E-SBC • Mediant 800 Gateway & E-SBC (Rev. B and C) • Mediant 1000B Gateway & E-SBC
Device	All products
Digital	Products with digital PSTN interfaces (ISDN BRI or PRI): • Mediant 500 Gateway & E-SBC • Mediant 500L Gateway & E-SBC • Mediant 800 Gateway & E-SBC (Rev. B and C) • Mediant 1000B Gateway & E-SBC
Mediant 90xx	• Mediant 9000 • Mediant 9000 Rev. B • Mediant 9030 • Mediant 9080
Mediant Software	Software-based products: • Mediant SE SBC • Mediant VE SBC • Mediant CE SBC

46

2 Latest Release (LR) Versions

This chapter describes new features, known constraints and resolved constraints of LR versions for Release 7.4.

2.1 Version 7.40A.100.233

This version includes new features and resolved constraints.

Note:

- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - 7.20A.260.*
  - 7.20A.258.*
  - 7.20A.256.*
  - 7.20A.204.878
  - 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx, Mediant VE/CE/SE SBCs:** Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - This version is compatible only with OVOC Version 8.0.1139 or later.
  - OVOC Version 8.0.1139 is compatible with both device versions 7.2 and 7.4.
  - If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.1139 or later prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to Version 8.0.1139 or later, prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

2.1.1 New Features

This section describes the new features introduced in this version.

2.1.1.1 Random String in Contact User Part for Re-Registrations

A new value (2) has been added to the existing [UseRandomUser] parameter, which enables the device to generate a randomized string for the user part of the Contact header for every sent SIP REGISTER message, including initial registrations as well as registration refreshes.

Applicable Application: All.

Applicable Products: All.

2.1.1.2 Session Expiry Observer Mode per RFC 4028

The device now complies strictly with RFC 4028 regarding SIP session expiration.

This feature is supported by the new [SipSessionExpiresObserverMode] global parameter, which determines if the observer mode (when IP Profile parameter 'Session Expires Mode' is configured to **Observer**) is strictly according to RFC 4028 or according to AudioCodes method of adding a "graceful" session expiration time.

Applicable Application: SBC.

Applicable Products: All.

2.1.1.3 New "Tenant ID" CDR Field

The CDR can now be customized in the SBC CDR Format table to include the Tenant ID, using a new CDR field called "Tenant ID". The Tenant ID value is obtained from any SIP header, using the new call variable *var.call.dst|src.TenantId* in Message Manipulation rules. This feature can be used to allow OVOC to know which Tenant ID the call belongs to.

Applicable Application: SBC.

Applicable Products: All.

2.1.2 Resolved Constraints

This section lists resolved constraints.

Table 2-1: Resolved Constraints in Version 7.40A.100.233

Incident	Description
SBC-29859	The device crashes (resets) when loading an incremental ini file that contains only NGINX configuration. Applicable Products: All
SBC-29860	The device fails to complete DTLS negotiation due to fragmented DTLS packets and as a result, the call fails. Applicable Products: All
SBC-30243	The device does not print the source/destination sub-addresses (if exist) in the "pstn recv <-- INCOMING_CALL" syslog message. Applicable Products: Gateway
SBC-30289	The device fails to add the Content-Disposition header to a SIP INFO request, as configured by the Message Manipulation. Applicable Products: All

Incident	Description
SBC-30368	The device rejects the SDP offer when it contains an "@" in the origin field ('o='), with a SIP 415 response and parsing error. As a result, the call fails. Applicable Products: All
SBC-30433	The device's web parameter 'Classify By Proxy Set Mode' should be under SIP Definitions General Settings > SBC Settings (instead of SIP Definitions General Settings > General). Applicable Products: All
SBC-30987	The device crashes (resets) with the exception reason "TPAPP no sched for the last 16000 ticks". Applicable Products: All
SBC-31143	The device fails to perform alternative routing when forking to two User-type IP Groups. As a result, the call fails. Applicable Products: All
SBC-31148	The device generates new user part for the Contact header in outgoing SIP 18x requests when the UseRandomUser parameter is configured to 2 (should only be generated for REGISTER messages). As a result, the call fails. Applicable Products: All
SBC-31177	The device sends RTP to the wrong port on simultaneous ring call flow, causing a one-way voice. Applicable Products: All
SBC-31236	The device tries to add the crypto suits group before removing the unsupported crypto suits, causing the call to fail. Applicable Products: All
SBC-31246	The device sends an alarm without indicating the severity level in REST API, for running an active DR rule. Applicable Products: All

2.2 Version 7.40A.100.114

This version includes new features and resolved constraints.

Note:

- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to this 7.4 version:

- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - 7.20A.260.*
  - 7.20A.258.*
  - 7.20A.256.*
  - 7.20A.204.878
  - 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx, Mediant VE/CE/SE SBCs:** Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:

- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - This version is compatible only with OVOC Version 8.0.1122 or later.
  - OVOC Version 8.0.1122 is compatible with both device versions 7.2 and 7.4.
  - If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.1122 or later prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to Version 8.0.1122 or later, prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

47

2.2.1 New Features

This section describes the new features introduced in this version.

2.2.1.1 NGINX Version Update

The device's embedded NGINX engine has been updated to Version 1.20.1.

Applicable Application: SBC

Applicable Products: All.

2.2.1.2 Mediant VE and CE Support for Gen3 Xeon-SP ("Ice Lake-SP")

The virtual SBCs (Mediant VE and CE) now support 3rd Gen Intel® Xeon® Scalable processors (code-named "Ice Lake-SP") based host servers. This allows the use of Intel's latest CPU server architecture with these SBCs.

Currently, there is no change in the supported SBC capacity when using these servers.

Applicable Application: SBC.

Applicable Products: Mediant VE; Mediant CE.

2.2.1.3 Secured Media Cluster Connectivity

Up until now, connectivity in the media cluster between the Signaling Component and the Media Components for the management of the Media Components was non-secured (TCP). Now, when upgrading to Version 7.40A.100.114, this connectivity changes to secured (TLS), by default. The connectivity mode can be configured (secured or non-secured), using the new [TpncpEncryptionEnable] parameter. For more information, refer to the *User's Manual*.

Applicable Application: SBC.

Applicable Products: Mediant VE; Mediant CE.

2.2.1.4 New SNMP Alarms

The following new SNMP alarms have been introduced in this version:

- acFaultyDSPAlarm - sent when one or more of the device's DSP cores are faulty.
- acTLSCertificateMismatchAlarm - sent when a mismatch occurs between the private key and the TLS certificate (public key).
- acMCNotSecuredAlarm – (Mediant VE/CE Only) sent when the connection between the Signaling Component (SC) and at least one of the Media Components (MC) remains unsecured after a specific partially completed upgrade scenario.

Applicable Application: All.

Applicable Products: All.

2.2.1.5 Mediant 9080 SBC Hardware Revision Update

Later this year, Mediant 9080 SBCs will be shipped with a new hardware revision that includes an updated CPU module.

There is no change in the Mediant 9080 supported capacity, device configuration or supported features following this update.

The updated hardware revision is supported by this 7.4 software version (7.40A.100.114) or later. Earlier 7.4 software versions are not compatible with the new hardware revision.

Support for the new hardware revision was also added to the 7.2 LTS software version stream (7.20A.258.661 or later).

For upgrading 7.2 software to 7.4, an intermediate version which supports the new hardware revision should be used (7.40A.005.569 or later). For the upgrade procedure, refer to *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

Note: **For Mediant 9080 HA system deployments:** The HA pair (active-redundant) can have different hardware revisions, only if they are both running a supported software version (see above). Therefore, Customers are recommended to consider upgrading their HA pair to a software version supporting the new hardware revision. Doing so will ensure that a Mediant 9080 with the new hardware revision can be used in the HA system in case of a need for device replacement.

The updated hardware revision can be identified using one of the following methods:

- Yellow label on the left side of the device's chassis:
  - **Previous HW revision:** "Version P01"
  - **Updated HW revision:** "Version P02"
- Silver label on the upper cover of the device's chassis:
  - **Previous HW revision:** "FPRZ00157" (AC power supply) or "FPRZ00168" (DC power supply)
  - **Updated HW revision:** "FPRZ00191" (AC power supply) or "FPRZ00192" (DC power supply)
- Using the CLI command `show system hardware`:
  - **Previous HW revision:** `CPU: Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz, total 48 cores, avx supported`
  - **Updated HW revision:** `CPU: Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz, total 64 cores, avx supported`

Note: Mediant 9030 SBCs and the old Mediant 9000 (Gen 8) SBCs are not affected by this update.

Applicable Application: SBC.

Applicable Products: Mediant 9080

2.2.1.6 Classify by Proxy Set using IP Address in SIP Contact Header

Up until now, the IP Group table's 'Classify By Proxy Set' parameter enabled the classification of incoming calls as belonging to a specific IP Group, by searching the associated Proxy Set for an IP address that matched the source IP address (ISO Layer 3) of the incoming packet.

Classification by Proxy Set can now be done using the IP address of the Contact header of the incoming SIP message. If the header contains a SIP URI that has an IP address in the host part that matches an IP address in the Proxy Set, the call is classified to the IP Group. This mode is useful, for example, when the source IP address is an internal address (like when the Mediant CE SBC is deployed in Azure).

To support this feature, a new global parameter—'Classify By Proxy Set Mode' (ClassifyByProxySetMode)—has been introduced, which determines the IP address used for this classification process - source IP address (default), IP address of Contact header, or both. When configured for both, the device first checks the associated Proxy Set for an IP address that matches the source IP address. If there is no match, it checks the Proxy Set for an IP address that matches the IP address of the Contact header.

Note:

- Classification using the Contact header is supported only when the header has an IP address (not a DNS hostname).

- For IDS, only the source IP address is used.
- For TLS Contexts, only the source IP address is used. (If a Proxy Set is not found, the TLS Context configured for the SIP Interface is used.)

Applicable Application: SBC.

Applicable Products: All.

2.2.1.7 SDR Fields for MOS

The device can now generate Session Detail Records (SDR) with Mean Opinion Score (MOS) fields, if customized to do so. These fields are generated at the end of the call (STOP SDRs) and indicate MOS values for incoming (local and remote peer) and outgoing (local and remote peer) calls:

- IngressLocalMosCQ
- IngressRemoteMosCQ
- EgressLocalMosCQ
- EgressRemoteMosCQ

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.2.2 Resolved Constraints

This section lists resolved constraints.

Table 2-2: Resolved Constraints in Version 7.40A.100.114

Incident	Description
SBC-28750	The device crashes (resets) upon a flash-hook in the middle of dialing a secondary call. Applicable Products: Gateway
SBC-28955	The device crashes (resets) upon ARM sending a discover remote hosts for service that has an illegal HOST line for ARMTopology. Applicable Products: All
SBC-29025	When the device is deployed on Microsoft Azure and undergoes an HA switchover, it loses connection with ARM. Applicable Products: Mediant CE
SBC-29358	The device doesn't update Contact details during registration in its registration database. Applicable Products: All
SBC-29386	The device ignores a SIP ACK for a SIP 302 response when it terminates an incoming INVITE using the internal and 302 response. As a result, call failure occurs. Applicable Products: All
SBC-29596 / SBC-29625	The device drops all pending retransmissions when receiving an ICMP error. Applicable Products: All
SBC-29604	The device sends a TLSCertificateMismatchAlarm alarm for the Media Component (MC). Applicable Products: Mediant CE

Incident	Description
SBC-29607 / SBC-30005	The device fails to load a TLS certificate, printing "RsaKeyMatch failed". Applicable Products: All
SBC-29614 / SBC-29822	The device's Web interface does not allow the user to change the index number of a row for a configuration table. Applicable Products: All
SBC-30080	The device's performance monitoring polling from OVOC fails when using a negative UTC offset (-1 or less). Applicable Products: All

48

2.3 Version 7.40A.100.021

This version includes only resolved constraints.

Note:
- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to this 7.4 version:
- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - 7.20A.260.*
  - 7.20A.258.*
  - 7.20A.256.*
  - 7.20A.204.878
  - 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx, Mediant VE/CE/SE SBCs:** Upgrade from Version 7.2 requires the use of a software image or an ISO file. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:
- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - This version is compatible only with OVOC Version 8.0.114 or later.
  - OVOC Version 8.0.114 is compatible with both device versions 7.2 and 7.4.
  - If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.114 or later prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to Version 8.0.114 or later, prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

2.3.1 Resolved Constraints

This section lists resolved constraints.

Table 2-3: Resolved Constraints in Version 7.40A.100.021

Incident	Description
-	The device doesn't support AWS. (Now supports AWS.) **Applicable Products:** Mediant Software
SBC-28951	When running on AWS, HA fails to initialize due to the wrong time zone in initial startup on the redundant unit. **Applicable Products:** Mediant Software
SBC-29207	When running on AWS, the device crashes (resets) on task "WEBS" because of wrong pointers to the HTTP Remote Host (ARM). **Applicable Products:** SBC
SBC-29365	When running on Hyper-V, the device loses voice when using VLAN tagging. **Applicable Products:** Mediant Software

2.4 Version 7.40A.100.011

This version includes new features, known constraints and resolved constraints.

Note:
- Mediant VE/CE SBC on AWS or Google Cloud are currently **not** supported in this version.
- FIPS Mode is not supported in this version.

Note: Upgrading from Version 7.2 to Version 7.40A.100.011:
- **For Mediant 90xx, Mediant VE/CE/SE SBCs:** For upgrade instructions, please refer to the document Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note.
- **For MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** These devices can be directly upgraded only from the following 7.2 versions:
  - 7.20A.260.*
  - 7.20A.258.*
  - 7.20A.256.*
  - 7.20A.204.878
  - 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.

Note:
- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - This version is compatible only with OVOC Version 8.0.114 or later.
  - OVOC Version 8.0.114 is compatible with both device versions 7.2 and 7.4.
  - If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.114 or later prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to Version 8.0.114 or later, prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

2.4.1 New Features

This section describes the new features introduced in this version.

2.4.1.1 MOS Measurement, Reporting and Storing per Registered User

The device can be configured to measure and report MOS (value and color) for users that are registered with the device:

- The SBC Registered Users table (and output of the CLI command `show voip register db sbc`) now displays MOS per registered user (stores MOS).
- The device can be configured to switch to a different voice coder (e.g., from G.7.11 to Opus) for new calls if the MOS of a registered user falls under a specific level.
- The device reports MOS to registered users, by sending an out-of-dialog SIP NOTIFY message containing the proprietary x-VoiceQuality header, at the end of the call.

To support this feature, the following configuration updates were made:

- New web page called Registered User Voice Quality (Setup menu > Signaling & Media tab > Media folder > Quality of Experience > Registered User Voice Quality), which provides the following new parameters:
  - 'Registered User MOS Observation Window': Defines the length (1 or 2 hours) of each interval in the "observation window" (12 intervals) for calculating average MOS.
  - 'MOS Stored Timeout For No Calls': Defines the period of no calls after which the MOS measurement is reset (0 with color gray).
- New IP Group table parameter 'User Voice Quality Report': Enables this feature for registered users belonging to the IP Group (User-type).
- New optional value **Registered User Voice Quality** for the 'Rule Metric' parameter in the Quality of Service Rules table: Defines the rule for this feature (reject calls or use an alternative IP Profile if MOS is low).

Note: For HA systems, upon an HA switchover, MOS measurements restart on the new active device.

Applicable Application: SBC.

Applicable Products: All.

2.4.1.2 MOS Measurement Based on RTCP

The device can calculate MOS based on RTCP without the need for RTCP-XR packets. This is useful for WebRTC calls since, up until now, MOS calculation wasn't available as WebRTC clients typically don't send RTCP-XR reports.

Applicable Application: All.

Applicable Products: Mediant 800; Mediant 2600; Mediant 4000; Mediant 90xx; Mediant Software.

49

2.4.1.3 Test Call Duration Specified in SIP INVITE

The duration of test calls can now be determined by the caller SIP user agent (UA). This is specified using the 'duration=<length in msec>' URI parameter of the Request-URI in the incoming SIP INVITE message. Up until now, caller-based test calls lasted until the caller ended the call (i.e., sent SIP BYE message).

This feature is in accordance with RFC 4240 (Basic Network Services with SIP).

This feature is also used for the MOS reporting of WebRTC click-to-call platforms feature, described in MOS Reporting for WebRTC Click-to-Call.

Applicable Application: All.

Applicable Products: All.

2.4.1.4 MOS Reporting for WebRTC Click-to-Call

The device can be configured to test voice quality (MOS) with WebRTC clients.

The test is typically triggered when a client accesses the web page on which the WebRTC click-to-call widget button is displayed. If the device reports a low MOS, Customers can, for example, have the button deactivated (grayed out) so that the client can't use it to call.

Implementation of this feature requires configuration on the device, and configuration by the Web Developer using AudioCodes WebRTC web browser client SDK API:

- AudioCodes WebRTC Web Browser Client SDK API:

  When the client opens the web page, the web browser needs to send the device a SIP INVITE message containing AudioCodes proprietary SIP header, 'X-AC-Action: test-voice-quality' and the 'duration=' parameter in the Request-URI. The device identifies this feature by the receipt of the 'X-AC-Action: test-voice-quality' header. The 'duration=' parameter specifies the duration of the test call (see Test Call Duration Specified in SIP INVITE). For more information on AudioCodes web browser client SDK API, click here.
- SBC Device:

  The device routes the incoming SIP INVITE from WebRTC client to its embedded Test Call endpoint and establishes the call. During the call, the device plays a pre-recorded tone (PRT) to the client. When the duration, specified in the Request-URI (see above) expires, the device terminates the call and sends a SIP BYE message containing AudioCodes proprietary SIP header, 'X-VoiceQuality'. This header indicates the measured MOS (value and color), for example, 'X-VoiceQuality: 42 green'.

Applicable Application: SBC.

Applicable Products: Mediant 800; Mediant 2600; Mediant 4000; Mediant 90xx; Mediant Software.

2.4.1.5 Enhanced Display of SBC Registered Users

The SBC Registered Users table, which displays users registered with the device, has been re-designed to provide the following enhancements:

- Capability to search for AORs (by user part)
- Display of number of registered AORs
- Display of a detailed information pane per contact of an AOR
- Improved readability

Applicable Application: SBC.

Applicable Products: All.

2.4.1.6 Capacity Increase of Configuration Tables

Capacity related to the following tables has been increased:

- Call Setup Rules table:
  - Max. rows:
    - Mediant 500/500L/800: 100
    - Mediant 1000/MP-1288: 64
    - Mediant 2600/4000: 400
    - Mediant 90xx/SE: 1,000
    - Mediant VE/CE: 500 for 2-8 GB and 1,000 for 16-64 GB
  - Max 'Rules Set ID's:
    - Mediant 500/500L/800/1000/MP-1288: 32
    - Mediant 2600/4000: 50
    - Mediant 90xx/SE: 100
    - Mediant VE/CE: 50 for 2-8 GB and 100 for 16-64 GB
  - Max. rules per 'Rules Set ID':
    - Mediant 500/500L/800/2600/4000/90xx/Software: 25
    - Mediant 1000/MP-1288: 10
- Accounts table:
  - Max Accounts per 'Served IP Group'
    - Mediant 500/500L/800: 30
    - Mediant 1000/MP-1288: 10
    - Mediant 2600/4000: 75
    - Mediant 90xx/SE: 100
    - Mediant VE/CE: 50 for 2-8 GB and 100 for 16-64 GB
- Message Manipulations table:
  - Max. 'Manipulation Set ID's:
    - Mediant 500/500L/800: 30
    - Mediant 1000/MP-1288: 20
    - Mediant 2600/4000: 50
    - Mediant 90xx/SE: 100
    - Mediant VE/CE: 50 for 2-8 GB; 100 for 16-64 GB
  - Max. rules per 'Manipulation Set ID':
    - Mediant 500/500L/800: 200
    - Mediant 1000/MP-1288: 100
    - Mediant 2600/4000: 500
    - Mediant 90xx/SE: 1,000
    - Mediant VE/CE: 750 for 2-8 GB; 1,000 for 16-64 GB

Applicable Application: All.

Applicable Products: All.

2.4.1.7 OpenSSL Updated to Version 1.1.1i

OpenSSL, which is implemented in AudioCodes devices for secure communication using TLS, has been updated to OpenSSL Version 1.1.1i.

Applicable Application: All.

Applicable Products: All.

2.4.1.8 SHA-2 Authentication Protocol for SNMPv3 Users

SNMPv3 users can now be configured with SHA-2 authentication (SHA-2 224-bit, SHA-2 256-bit, SHA-2 384-bit, and SHA-2 512-bit). Up until now, only MD5 and SHA-1 were supported. This feature is configured by the existing 'Authentication Protocol' parameter in the SNMPv3 Users table.

Applicable Application: All.

Applicable Products: All.

2.4.1.9 SNMP Enabled and Disabled On-The-Fly

A device reset is no longer required after changing the value of the 'Disable SNMP' parameter for enabling or disabling SNMP.

Applicable Application: All.

Applicable Products: All.

2.4.1.10 New Default TLS Version

For enhanced security, the default value of the 'TLS Version' parameter in the TLS Contexts table has been changed from **Any TLS1.x** (0), which includes the relatively weak TLS versions 1.0 and 1.1, to **TLSv1.2 and TLSv1.3** (12).

Applicable Application: All.

Applicable Products: All.

2.4.1.11 SRTCP per IP Profile

Up until now, Secure RTCP (SRTCP) packet encryption could only be configured globally (all calls), using the 'Encryption on Transmitted RTCP Packets' [RTCPEncryptionDisableTx] parameter. In other words, both legs of the call could only be enabled or disabled for SRTCP. Now, SRTCP can be configured per specific calls using the new IP Profile parameter 'Encryption on RTCP Packets', allowing different settings for the incoming and outgoing legs (e.g., enabled for the incoming leg and disabled for the outgoing leg).

Applicable Application: SBC.

Applicable Products: All.

2.4.1.12 SRTP Crypto Suites per IP Profile

Supported offered crypto suites for SRTP can now be configured per IP Profile. Up until now, crypto suites (all or only one) could only be configured globally (for all calls), using the 'Offered SRTP Cipher Suites' parameter (which is still the default if not configured by this new feature).

This feature is configured by the following:

- New table - SBC Crypto Suite Groups (Setup menu > Signaling & Media tab > Media folder > SBC Crypto Suite Groups), which defines groups of crypto suites (AES-CM-128-HMAC-SHA1-80, AES-CM-128-HMAC-SHA1-32, AES-256-CM-HMAC-SHA1-80 and/or AES-256-CM-HMAC-SHA1-32)
- New IP Profile parameter 'Crypto Suites Group', which assigns an SBC Crypto Suite

Group to the IP Profile

Applicable Application: SBC.

Applicable Products: All.

2.4.1.13 Additional SSH Settings for Secure CLI

Secure access to the device's CLI through SSH has been enhanced by the following new SSH configuration parameters:

- [SSHKexAlgorithmsString]: Key Exchange Method (Diffie-Hellman-Group-Exchange-SHA256 or Diffie-Hellman-Group1-SHA1)
- [SSHCiphersString]: Cipher string (AES128-CTR or AES128-CBC)
- [SSHMACsString]: HMAC (HMAC-SHA2-256 or HMAC-SHA1)

Applicable Application: All.

Applicable Products: All.

2.4.1.14 Prefer Secured Media on Outgoing SDP Answer

The device can now be configured to prefer secured media on the outgoing SDP answer sent by the device. When configured and a peer SIP user agent offers both secured and unsecured media, the device chooses to use secured media (SRTP).

This feature is supported by configuring the existing IP Profile parameter 'SBC Media Security Mode' to the new optional value, **Offer Both - Answer Prefer Secured** (4).

Applicable Application: SBC.

Applicable Products: All.

2.4.1.15 LDAP Authentication for NGINX HTTP Reverse Proxy

The device's HTTP Reverse Proxy can now be configured to authenticate HTTP requests with an LDAP server.

Applicable Application: All.

Applicable Products: All.

2.4.1.16 Enhanced NGINX Support for TLS Context Parameters

The device's integrated NGINX server supports the following additional parameters in the TLS Contexts table: 'Cipher Server TLS1.3', 'Cipher Client TLS1.3', 'Key Exchange Groups', 'Strict Certificate Extension Validation', and 'DH key Size'.

Applicable Application: All.

Applicable Products: All.

2.4.1.17 HTTP Proxy Interface Binding to Device Network Interface

The device's embedded NGINX can be enabled to bind the HTTP Proxy interface to a specific device network interface. This feature is configured by the new 'Bind To Device' parameter (enable/disable) in the HTTP Proxy Servers table.

Applicable Application: SBC.

Applicable Products: All.

SO

2.4.1.18 Case-Sensitivity for Dial Plan Matching

Matching Dial Plan patterns can now be configured to take into account case-sensitivity (upper- or lower-case letters). This feature is configured by the new parameter, 'Prefix Case Sensitivity' in the Dial Plan table.

Applicable Application: All.

Applicable Products: All.

2.4.1.19 Conference Call Support with Microsoft Local Media Optimization

The device can now handle conference calls with Local Media Optimization for Microsoft Teams Direct Routing. If a call is established with a Teams user who wants to add a third-participant, Teams sends a SIP re-INVITE message to connect the new media. The device can handle this even if the initial user location is internal, by offering its public IP address (instead of its private IP address). The device does this by its additional support for handling X-MS headers received from the Teams client in re-INVITE messages. Using the re-INVITE, a non-direct media internal call (using the internal Media Realm) or a direct media call can be changed to non-direct media external call (using the regular Media Realm for the IP Group).

Applicable Application: SBC.

Applicable Products: All.

2.4.1.20 IPv6 for Debug Recording Server

The remote debug recording server (to where the device sends debug recording packets), can now be configured (by the existing DebugRecordingDestIP parameter) to an IPv6 address.

Applicable Application: All.

Applicable Products: All.

2.4.1.21 Enhanced Debug File Contents

The device's debug file now provides additional information of the device's configuration and status (e.g., date and memory). This information is located in the new *status.tar.gz* file.

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.4.1.22 Embedded RPCAP Server for Packet Capturing

The device now provides an embedded Remote Capture Protocol (rpcap) server that allows Wireshark to connect to it remotely. Once connected, Wireshark controls the packet capturing process (i.e., starting/stopping network capture of selected network interfaces, collecting the captured data, and filtering it). For more information on rpcap functionality, refer to Wireshark documentation.

The device's rpcap server is enabled by the new CLI command, `debug capture rpcap-server [start|stop] [<port number>]`. By default, the device use port 2002 for the remote packet capture sessions.

Applicable Application: All.

Applicable Products: All.

2.4.1.23 Persistent Storage of History Alarms

SNMP alarms in the Alarms History table can now be stored on the device's flash memory and maintained (persistent) even after a device reset. Up until now (and when the feature is disabled), these alarms are deleted from the table upon a device reset.

This feature is configured by the following new parameters:

- [AlarmsPersistentHistory]: Enables the feature. When enabled, the Alarms History page displays an additional column called "Note", which indicates if the alarm occurred (raised or cleared) before or after the last device restart.
- [SavePersistentHistoryInterval]: Defines how often the device saves the alarms of the Alarms History table to flash (overwriting previously stored file).

Note: Currently, the device cannot be connected to OVOC when this feature is enabled.

Applicable Application: All.

Applicable Products: All.

2.4.1.24 SDR Enhancements

The Session Detail Record (SDR) feature has been enhanced:

- The device can now generate a new SDR type called "INTERMEDIATE". These SDRs are generated during the call. The time when the first Intermediate SDR is generated is configurable, by the new parameter 'First Intermediate Interval'. The interval between every generated SDR during the call is also configurable, by the new parameter 'Periodic Intermediate Interval'.
- Additional fields (optional) have been added to the SDR (media-related and tag fields)

Applicable Application: All.

Applicable Products: Mediant 90xx; Mediant Software.

2.4.1.25 New Performance Monitoring Parameters

The device's Performance Monitoring module has been enhanced with additional performance monitoring parameters, providing statistical information for the following:

- WebRTC sessions and license key usage
- DS-1 (T1) calls
- Analog calls
- Storage utilization
- CPU utilization
- Call sessions
- Transcoding sessions
- Various SIP (SUBSCRIBE and REGISTER)
- DDOS

Applicable Application: All.

Applicable Products: All.

2.4.1.26 IP Profile Used by Third-Party Routing Server or ARM

IP Profiles can now be configured to be used by third-party routing servers or AudioCodes ARM. This feature is configured by the new IP Profile parameter, 'Used By Routing Server'.

Applicable Application: All.

Applicable Products: All.

2.4.1.27 Change in 'Caller ID Transport Type' Parameter Behavior

The 'Caller ID Transport Type' parameter [CallerIDTransportType] has been modified. The optional value **Relay** (1) is no longer supported and a new optional value **Set By Software** (4) has been added (which is now the new default value).

When the parameter is configured to **Set By Software**, Gateway calls will use the caller ID behavior as though the parameter is configured to **Mute** (3), and SBC calls will use the caller ID behavior as though the parameter is configured to **Disable** (0).

Applicable Application: All.

Applicable Products: MP-1288; Mediant 500; Mediant 500L; Mediant 800; Mediant 1000.

2.4.1.28 Missing Commands and Web Parameters Added

The following CLI commands and Web parameters (fields) that were missing in previous versions have now been added.

- New CLI commands:
  - `digest-auth-uri-mode` [SipDigestAuthorizationUriMode]
  - `unreg-on-startup` [UnRegisterOnStartup]
  - `max-sdp-sess-ver-id` [MaxSdpSessionVersionId]
  - `regions-connectivity-dial-plan` [RegionsConnectivityDialPlan]
  - `deny-access-on-fail-count` [DenyAccessOnFailCount]
  - `deny-auth-timer` [DenyAuthenticationTimer]
  - `use-rand-user` [UseRandomUser]
- New Web fields (TLS Contexts > Change Certificates table):
  - 'Subject Key Identifier' (`set-subject-key-identifier`)
  - 'Key Usage' (`set-key-usage`)
  - 'Extended Key Usage' (`set-extended-key-usage`)

Applicable Application: All.

Applicable Products: All.

2.4.2 Known Constraints

This section lists known constraints.

Table 2-4: Known Constraints in Version 7.40A.100.011

Incident	Description
SBC-28846	If an Ethernet Device associated with an IPv6 network interface is modified, the associated Static Route is deleted. Applicable Products: All

2.4.3 Resolved Constraints

This section lists resolved constraints.

Table 2-5: Resolved Constraints in Version 7.40A.100.011

Incident	Description
SBC-28575	Loading certificate errors appear in the Syslog. Applicable Products: All
SBC-27683	The device crashes (resets) on networking task (signal 904, task NWST). Applicable Products: Mediant 1000
SBC-27283	Removing Calling Name towards PSTN also removes Facility IE [03], causing the ISDN side to not recognize the reason of Anonymous call. As a result the call fails. Applicable Products: Gateway
SBC-27189	The device sends connection line 'c=0.0.0.0' in the SDP if it receives an SDP offer with a 'c=' line in the session section and an SDP answer with a 'c=' line in the media section. As a result, one-way voice occurs. Applicable Products: All
SBC-25947	SSH weakness discovered by the pentest tool. Applicable Products: All
SBC-25560	No corresponding CLI command for the ini file parameter [UseRandomUser]. Applicable Products: All
SBC-25064	The device fails to activate GenerateRTP (no voice) after call transfer Applicable Products: All
SBC-18309	The device saves only the first 20 coders in the SDP offer, causing a DTMF miss-match. Applicable Products: All
SBC-27859 / SBC-27894 / SBC-28131	A CPU overload of 100% is caused by a failed networking task. Applicable Products: All
25546 / 25157	When the Dial Plan is configured with the "n" wildcard, it doesn't only match digits 2 to 9. Applicable Products: All
22858	NGINX doesn't support the following TLS Context parameters - Cipher Server TLS13, Cipher Client TLS13, Key Exchange Groups Applicable Products: All

S1

2.5 Version 7.40A.005.613

This version includes new features, known constraints and resolved constraints.

Note:
- Mediant VE/CE SBC on Google Cloud are currently **not** supported in this version.
- For FIPS support, please contact AudioCodes for details.

Note: Upgrading from Version 7.2 to this 7.4 version:
- Upgrade to Version 7.4 can only be done from the following 7.2 versions:
  - 7.20A.260.*
  - 7.20A.258.*
  - 7.20A.256.*
  - 7.20A.204.878
  - 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that the device is running one of these 7.2 versions.
- **Mediant 90xx, Mediant VE/CE/SE SBCs:** Upgrade from Version 7.2 requires the use of a software image or an ISO file. Hitless upgrade requires the use of the "intermediate" 7.40A.005.509 version. For upgrade instructions, refer to the document *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.
- **MP-1288, Mediant 500, Mediant 500L, Mediant 800, Mediant 1000, Mediant 2600, Mediant 4000 SBCs:** Upgrade from Version 7.2 is done with the 7.4 .cmp file using the regular Software Upgrade Wizard method.

Note:
- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - This version is compatible only with OVOC Version 8.0.1122 or later.
  - OVOC Version 8.0.1122 is compatible with both device versions 7.2 and 7.4.
  - If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.1122 or later prior to upgrading your device to this SBC version.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to Version 8.0.1122 or later, prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

2.5.1 New Features

This section describes the new features introduced in this version.

2.5.1.1 Mediant VE and CE Support for Gen3 Xeon-SP ("Ice Lake-SP")

The virtual SBCs (Mediant VE and CE) now support 3rd Gen Intel® Xeon® Scalable processors (code-named "Ice Lake-SP") based host servers. This allows the use of Intel's latest CPU server architecture with these SBCs.

Currently, there is no change in the supported SBC capacity when using these servers.

Applicable Application: SBC.

Applicable Products: Mediant VE; Mediant CE.

2.5.1.2 Mediant 9080 SBC Hardware Revision Update

Later this year, Mediant 9080 SBCs will be shipped with a new hardware revision that includes an updated CPU module.

There is no change in the Mediant 9080 supported capacity, device configuration or supported features following this update.

The updated hardware revision is supported by this 7.4 software version (7.40A.100.114) or later. Earlier 7.4 software versions are not compatible with the new hardware revision.

Support for the new hardware revision was also added to the 7.2 LTS software version stream (7.20A.258.661 or later).

For upgrading 7.2 software to 7.4, an intermediate version which supports the new hardware revision should be used (7.40A.005.569 or later). For the upgrade procedure, refer to *Mediant SW and 90xx SBC Upgrade Procedure from 7.2 to 7.4 Configuration Note*.

Note: **For Mediant 9080 HA system deployments:** The HA pair (active-redundant) can have different hardware revisions, only if they are both running a supported software version (see above). Therefore, Customers are recommended to consider upgrading their HA pair to a software version supporting the new hardware revision. Doing so will ensure that a Mediant 9080 with the new hardware revision can be used in the HA system in case of a need for device replacement.

The updated hardware revision can be identified using one of the following methods:

- Yellow label on the left side of the device's chassis:
  - **Previous HW revision:** "Version P01"
  - **Updated HW revision:** "Version P02"
- Silver label on the upper cover of the device's chassis:
  - **Previous HW revision:** "FPRZ00157" (AC power supply) or "FPRZ00166" (DC power supply)
  - **Updated HW revision:** "FPRZ00191" (AC power supply) or "FPRZ00192" (DC power supply)

- Using the CLI command `show system hardware`:
  - **Previous HW revision:** `CPU: Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz, total 48 cores, avx supported`
  - **Updated HW revision:** `CPU: Intel(R) Xeon(R) Gold 6226P CPU @ 2.90GHz, total 64 cores, avx supported`

Note: Mediant 9030 SBCs and the old Mediant 9000 (Gen 8) SBCs are not affected by this update.

Applicable Application: SBC.

Applicable Products: Mediant 9080

2.5.2 Known Constraints

This section lists known constraints.

Table 2-6: Known Constraints in Version 7.40A.005.613

Incident	Description
SBC-30961	Media performance monitoring statistics (e.g., mediaKBytesInTotal) for calls that were established prior to an HA switchover and then closed after the switchover are not calculated in the new active device. Applicable Products: All

2.5.3 Resolved Constraints

This section lists resolved constraints.

Table 2-7: Resolved Constraints in Version 7.40A.005.613

Incident	Description
SBC-17014	A mismatch exists between the Performance Monitoring parameter and the CDR for attempted calls count. Applicable Products: All
SBC-18552	When the IP Group name is modified, the active alarm is not updated to reflect this name change. Applicable Products: All
SBC-19449	The device crashes (resets) when a search is performed in the Web interface that has a result of more than 3,000 characters. Applicable Products: All
SBC-19692	The device fails to perform a Telnet connection from the active to redundant unit. Applicable Products: HA
SBC-29907	Performance Monitoring polling from OVOC fails upon an NTP refresh. Applicable Products: All
SBC-29951	Performance Monitoring polling from OVOC fails upon negative UTC offsets other than -1. Applicable Products: All
SBC-30187	The device crashes (resets) with the error "TASK SPMR" due to race condition. Applicable Products: All

Incident	Description
SBC-30383	The device crashes (resets) with the exception reason "TPAPP no sched for the last 16000 ticks". Applicable Products: All
SBC-31090	A CPU overload of 100% is caused by a failed networking task. Applicable Products: All

S2

2.6 Version 7.40A.005.509

This version includes new features and resolved constraints.

Note: Mediant VE/CE SBC on Google Cloud is currently **not** supported in this version.

Note:

- **This version supports device upgrade from the following 7.2 versions:**
  - 7.20A.260.*
  - 7.20A.258.*
  - 7.20A.256.*
  - 7.20A.204.878
  - 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that you are using one of the supported versions listed above.
- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - This version is compatible only with OVOC Version 8.0.114 or later.
  - OVOC Version 8.0.114 is compatible with both device versions 7.2 and 7.4.
  - If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 8.0.114 or later prior to upgrading your device to this SBC version.
  - For Mediant VE/CE on Azure or AWS, the device serial number changes during the upgrade from Version 7.2 to 7.4 and therefore, a new entity for the device is created on OVOC. This limitation will be resolved in OVOC Version 8.0.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to Version 8.0.114 or later, prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

2.6.1 New Features

This section describes the new features introduced in this version.

2.6.1.1 Disk Resize for Mediant VE

By default, Mediant VE images in Version 7.4 use 20 GB disk size. If additional disk space is needed, the virtual machine's disk size can be changed through the virtual environment / public cloud configuration. For example, in Azure it's done via the Azure Portal by navigating to **Disks** > disk_name > **Size + performance**, and then choosing **Resize**. Mediant VE software adjusts itself to the new disk size upon the next reboot.

Applicable Application: SBC

Applicable Products: Mediant VE.

2.6.1.2 Support for Mediant VE SBC on Hyper-V and KVM

Mediant VE is now supported by Version 7.4 on Hyper-V and KVM platforms.

Applicable Application: SBC

Applicable Products: Mediant VE.

2.6.2 Resolved Constraints

This section lists resolved constraints.

Table 2-8: Resolved Constraints in Version 7.40A.005.509

Incident	Description
SBC-19202	The device's Web interface is exposed to HTML code injection vulnerability. Applicable Products: All
SBC-22878	The device's NGINX configuration fails when IPv6 interfaces are used. Applicable Products: All
SBC-26515 / SBC-27917	The device responds to the REST `GET /api/v1/status` with the wrong time format in "localTimeStamp", causing loss of synchronization with OVOC. Applicable Products: All
SBC-27171	The device's hostname is missing in the textual description of the No-HA alarm and Manual Switch over alarm. Applicable Products: HA
SBC-27533	After upgrading Media Components to Version 7.4, the number of CPU cores is reduced from 8 to 7. Applicable Products: Mediant Software

2.7 Version 7.40A.005.314

This version includes new features, known constraints, and resolved constraints.

Note: The following products are **not** supported in this version and will be supported in the next applicable release:

- Mediant VE SBC on Hyper-V and KVM
- Mediant VE/CE SBC on Google Cloud

Note:

- **Version 7.4 supports device upgrade from the following 7.2 versions:**
  - 7.20A.260.*
  - 7.20A.258.*
  - 7.20A.256.*
  - 7.20A.204.878
  - 7.20A.204.549

  Therefore, prior to upgrading to Version 7.4, make sure that you are using one of the supported versions listed above.
- **Using this SBC version with AudioCodes One Voice Operations Center (OVOC):**
  - This version is compatible only with OVOC Version 7.8.2265 or later.
  - OVOC Version 7.8.2265 is compatible with both device versions 7.2 and 7.4.
  - If you plan on using OVOC with this SBC version, first upgrade your OVOC to version 7.8.2265 or later prior to upgrading your device to this SBC version.
  - For Mediant VE/CE on Azure or AWS, the device serial number changes during the upgrade from Version 7.2 to 7.4 and therefore, a new entity for the device is created on OVOC. This limitation will be resolved in OVOC Version 8.0.
- **Using this SBC version with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to Version 7.8.2265 or later, prior to upgrading the devices in the pool to this SBC version. Failure in doing so removes the 7.4 devices from the centralized license pool.

2.7.1 New Features

This section describes the new features introduced in this version.

2.7.1.1 CentOS Stream 8

Version 7.4 uses custom Linux distribution based on CentOS Stream 8.

For upgrading your SBC from the 7.20A stream (based on CentOS 6), refer to the document SBC Upgrade Procedure from Ver. 7.2 to 7.4 Configuration Note. For upgrading your SBC from the 7.20CO stream (based on CentOS 8), use the Web-based interface's Software Upgrade Wizard.

Note: For hitless upgrade from 7.20A steam versions, AudioCodes provides a CMP file for an intermediate 7.4 version based on CentOS 6. This intermediate version is intended **only** for temporary use during the upgrade process. For more information, refer to the document, *SBC Upgrade Procedure from Ver. 7.2 to 7.4 Configuration Note*.

Applicable Application: SBC

Applicable Products: Mediant VE; Mediant CE; Mediant SE; Mediant 9000.

2.7.1.2 SNMP and Telnet Protocols Disabled by Default

SNMP and Telnet protocols are disabled by default for improved device security.

If you want to use one of these protocols, enable them using the following configuration parameters:

- **SNMP:** Setup > Administration > SNMP > SNMP Community Settings > 'Disable SNMP'
- **Telnet:** Setup > Administration > Web & CLI > CLI Settings > 'Embedded Telnet Server'

Note: The SNMP protocol must be enabled for devices that are managed by AudioCodes One Voice Operations Center (OVOC).

Applicable Application: SBC

Applicable Products: Mediant VE; Mediant CE; Mediant SE; Mediant 90xx.

2.7.1.3 Performance Monitoring Graph Configuration through CLI

The performance monitoring graphs and KPI layouts can now also be configured through the device's CLI, using the new `configure system > kpi` command.

Applicable Application: SBC

Applicable Products: All.

2.7.1.4 Performance Monitoring for Dropped Packets due to Firewall

A new performance monitoring parameter (adDroppedTotal) has been added, which counts the number of IP packets dropped due to the device's Firewall table (access list).

Applicable Application: All

Applicable Products: All.

2.7.1.5 Syslog Messages to Serial Console

The device can now be configured to send syslog messages to the serial console (physically connected to the serial interface). This feature is enabled by the new parameter EnableConsoleLog (requires a device reset). The syslog messages are also sent to the remote Syslog server. While enabled, the CLI cannot be used for anything else.

Applicable Application: All

Applicable Products: All.

2.7.1.6 NGINX Version Update

The device's embedded NGINX engine has been updated to Version 1.19.1.

Applicable Application: SBC

Applicable Products: All.

2.7.2 Known Constraints

This section lists known constraints.

Table 2-9: Known Constraints in Version 7.40A.005.314

Incident	Description
SBC-27005 / SBC-23971	When terminating the ping through CLI, using the key sequence ^C, error messages appear in the Syslog and this action may crash (reset) the device. Applicable Products: Mediant 4000
SBC-27180	Software Upgrade from 7.20.CO.258.* versions is supported only via the Web Interface. Upgrade via REST API / CLI interface / Stack Manager is not working. Applicable Products: Mediant 90xx; Mediant VE; Mediant CE

2.7.3 Resolved Constraints

This section lists resolved constraints.

Table 2-10: Resolved Constraints in Version 7.40A.005.314

Incident	Description
SBC-24681	The device sends the debug file to the TFTP server from the wrong network interface. Applicable Products: All
SBC-24807	The device doesn't update the redundant unit after the license pool parameter is changed, causing an alarm. Applicable Products: HA
SBC-25108	The device resets with Task SPMT because of a memory overrun. Applicable Products: All
SBC-25197	The device's REST API has a syntax error for KPI (missing ":"). Applicable Products: All

Incident	Description
SBC-25548	The 'Condition' field in the Message Conditions table is limited to 200 characters. This bug has been resolved (increased to 299). Applicable Products: All
SBC-26699	The device loses its certificate after an HA switch over because of a disproportion of TLS Contexts between active and redundant units. Applicable Products: HA

2.8 Version 7.40A.002.007

This version includes new features, known constraints, and resolved constraints.

Note: The following products are not supported in this version and will be supported in the next applicable release:

- Mediant 9000 SBC
- Mediant 9030 SBC
- Mediant 9080 SBC
- Mediant SE SBC
- Mediant VE SBC
- Mediant CE SBC

Note:

- **Version 7.4 supports device upgrade from the following 7.2 versions:**
  - 7.20A.204.xxx software stream: 7.20A.204.540 and later
  - 7.20A.258.xxx software stream: 7.20A.258.119 and later
  - 7.20A.260.xxx software stream: 7.20A.260.005 and later

  Therefore, prior to upgrading to Version 7.4, make sure that you are using one of the supported versions listed above.
- **Using Version 7.4 with AudioCodes One Voice Operations Center (OVOC):**
  - This version is compatible only with OVOC Version 7.8.2000 or later.
  - OVOC Version 7.8.2000 is compatible with both device versions 7.2 and 7.4.
  - If you plan on using OVOC with SBC Version 7.4, first upgrade your OVOC to version 7.8.2000 or later prior to upgrading your device to Version 7.4.
- **Using Version 7.4 with a centralized license pool:**

  Customers using OVOC to manage their centralized license pool (Fixed, Floating, or Flex pool) must first upgrade their OVOC to Version 7.8.2000 or later, prior to upgrading the devices in the pool to Version 7.4. Failure in doing so removes the 7.4 devices from the centralized license pool.

2.8.1 New Features

This section describes the new features introduced in this version.

2.8.1.1 FIPS Support

The device can operate in "FIPS Mode" to fully comply with Federal Information Processing Standards (FIPS) 140-2 Level 1, which is a security standard specified by the United States Government that is used to validate cryptographic modules (i.e., the device). The FIPS standards specify best practices and security requirements for implementing crypto algorithms, encryption schemes, handling important data, and working with various operating systems and hardware, whenever cryptographic-based security systems must be used to protect sensitive, valuable data. FIPS also defines specific methods for encryption and specific methods for generating encryption keys. For more information on AudioCodes' FIPS certification, go to https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3708.

The following new CLI commands were added for enabling and configuring FIPS on the device:

- `fips on|off`: Enables and disables FIPS mode.
- `clear security-files`: Triggers zeroization (automatically done when enabling FIPS mode). Zeroization wipes out all sensitive content residing on the device, including security secrets such as private keys for SSH and TLS, the core dump file, and System Snapshot files.
- `show system security status`: Indicates if the device is operating in FIPS mode.

Applicable Application: SBC

Applicable Products: Mediant 9080; Mediant 4000B.

2.8.1.2 Enhanced DoS and DDoS Protection

The device provides improved protection from Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks:

- Enhanced prevention of DoS/DDoS SIP flood attacks
- Improved defense against TCP/IP vulnerabilities
- Optimal handling of SIP user registration avalanche
- Designed to prevent over-the-top traffic from unknown sources

Applicable Application: SBC

Applicable Products: Mediant 90xx; Mediant Software.

2.8.1.3 Lawful Interception Support

Note:

- The Lawful Interception feature is not part of the standard Software Version 7.4 build. It is delivered as a separate, dedicated 7.4 version build, available only to Customers that have ordered and licensed this feature.
- For further information on the Lawful Interception feature, contact your AudioCodes sales representative.

Under the terms stated in the note above, the device now supports lawful interception for intercepting signaling and media traffic of specific (targeted) subscribers towards mediation devices in Law Enforcement Agency (LEA) networks. This functionality is known as Lawful Interception and refers to the facilities in telecommunications and telephone networks that allow LEAs (with court orders or other legal authorization) to selectively wiretap individual subscribers.

Applicable Application: SBC

Applicable Products: Mediant 9080; Mediant VE/SE.

SH

2.8.1.4 New Performance Measurement Infrastructure

The device provides a new infrastructure for performance monitoring.

2.8.1.4.1 New Performance Measurement System

The device provides a new performance monitoring (PM) infrastructure, offering the following enhancements:

- Five-fold increase in the number of key-performance metrics (KPI), measuring almost every aspect of the SBC including additional areas such as license usage, DDOS, CPU utilization, and memory usage.
- Capability to configure a fully customized threshold-crossing SNMP trap event (acKpiThresholdCrossing / OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.148) per performance monitoring parameter and entity (e.g., per IP Group):
  - Threshold value to raise and clear the trap event
  - Trap severity level
  - Trap message
- Delivery of PMs to multiple interfaces, including REST API, SNMP, CLI, Web and OVOC. REST and CLI interfaces also enable the user to perform flexible queries of PMs (for example, for a specific measured interval), including the ability to query multiple concurrent PMs in a single request.
- Web interface provides a sophisticated tool for plotting graphs of performance monitoring parameters (real-time or historical). The graphs can be customized (labels, line color, and legend) and can be sent to a printer or downloaded in different file formats (e.g., PDF or PNG).
- Number of stored 15-minute collection intervals has been increased from 2 to 4 for historical PM measurements (some PMs have even been increased to a 100 – reflecting 25 hours).

Note: Due to this new performance monitoring system, the following previously supported features are now obsolete:

- Success/Failure Ratio page (Monitor menu > Monitor tab > Performance Monitoring folder > Success / Failure Ratio)
- Average Call Duration page (Monitor menu > Monitor tab > Performance Monitoring folder > Average Call Duration)
- Trunk Utilization page (Monitor menu > Monitor tab > Performance Monitoring folder > Trunk Utilization)
- Performance Profile table (Monitor menu > Monitor tab > Performance Monitoring folder > Performance Profile)
- User Defined Failure PM table (Monitor menu > Monitor tab > Performance Monitoring folder > User Defined Failure PM)

Applicable Application: All.

Applicable Products: All.

2.8.1.4.2 Plotting Graphs for Performance Monitoring Parameters

Performance monitoring parameters (real-time or historical) can now be displayed in the Web interface in graph format:

- Graphs can be displayed in different grid layouts per page (1x1, 1x2, 2x1, or 2x2).
- Graph title, x-axis title, and y-axis title can be customized.
- Each graph can include multiple, plotted performance monitoring parameters.
- Each plotted performance monitoring parameter can be assigned a line color, allowing

the user to easily distinguish between the performance monitoring parameters on the graph.

- A powerful, but easy-to-use tool is provided for drilling down and selecting each performance monitoring parameter from the device's hierarchical structure of REST-based performance monitoring parameters.
- A tooltip can be enabled which displays the value where the user hovers over the plotted performance monitoring line.
- Each graph provides a legend, showing the performance monitoring parameter's name and its color. The legend can also be used to filter the graph, by hiding or showing the plotted performance monitoring parameter.
- The graph can be easily zoomed in or out, allowing the user to view values of different resolutions.
- Graphs can be printed or downloaded in file format (PNG, JPEG, SVG, PDF or CSV).

The feature is configured by the following parent-child Web page, located under the new Monitor menu > Monitor tab > Performance Monitoring folder:

- Parent table (page) - KPI Layouts table: This table configures the layout's name and grid layout.
- Children pages: These are the pages of each configured KPI Layout, on which the actual graphs are created and plotted.

Applicable Application: All.

Applicable Products: All.

2.8.1.4.3 Alarm Thresholds for Performance Monitoring

Alarm thresholds (acKpiThresholdCrossing / OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.148) can now be configured for any performance monitoring parameter. An alarm can be configured to be raised or cleared when the parameter crosses a user-defined upper or lower threshold value. The alarm text of the raised or cleared alarm can also be customized as well as the severity level of the raised alarm.

The feature is supported by the new Alarm Thresholds table, located under Setup menu > Administration tab > Performance Monitoring folder.

Applicable Application: All.

Applicable Products: All.

2.8.1.5 Session Detail Records (SDR) Support

The device can now generate Session Detail Records (SDRs). Unlike CDRs, which are generated per SBC leg (ingress or egress leg of the call), SDRs are generated for both legs. In other words, an SDR is a call detail record of the entire call session. SDRs also contain more information on the call that is relevant for billing applications and thus, are especially useful in billing applications.

SDRs can be stored locally on the device in CSV format or periodically sent to a remote third-party SFTP server. The SDR can be generated for successfully established and terminated calls (STOP SDRs), or for failed call attempts (ATTEMPT SDRs).

The device supports a default SDR structure. However, the structure can be customized, by selecting only the fields to include in the SDR and by defining the field names (titles).

For SDR configuration, the Web interface's navigation pane provides a new "Session Detail Record" folder, which contains menu items that open the following new pages:

- SDR Settings page:
  - General:
    - 'Record Type'

  - Syslog SDR Reports:
    - 'SDR Syslog': Defines a dedicated Syslog server to where SDRs can be sent
    - 'SDR Server IP Address': Defines the address of the Syslog server (if not configured, sends to CDR Syslog server address)
  - SDR Local Storage:
    - 'Local Storage': Enables local storage of SDRs.
    - 'File Size': Defines the maximum size (in kilobytes) of the SDR file.
    - 'Number of files': Defines the maximum number of SDR files in local storage.
    - 'File name': Defines the filename format of the stored SDR file.
    - 'Rotation period': Defines how often an SDR file is created.
    - 'Compression format': Defines the file compression type (none, .zip, or .gzip).
  - SDR Servers:
    - 'SDR Servers Send Period': Defines the interval between each SDR files transaction to the server.
    - 'SDR Servers Bulk Size': Defines the number of files sent to the server at each file transfer transaction.
    - 'Pending SDR Files': Displays the number of files yet to be transferred.

    If the device fails to send the locally stored SDRs to the remote servers, the device sends a new SNMP alarm, acSDRServerAlarm (1.3.6.1.4.1.5003.9.10.1.21.2.0.147).
- SBC SDR Format table: This new table customizes the SDR fields (remove, add, or change the name of fields, change order of fields)
- SBC SDR Remote Servers table: Defines up to two remote SDR servers, which can provide active-standby redundancy.

For HA, SDR configuration is synchronized. For local storage, active and redundant devices maintain their own stored SDR files. Upon switchover, the stored files are not copied over. Stored files on the redundant device can be viewed and managed from the active device through SSH or SFTP.

Applicable Application: SBC.

Applicable Products: Mediant Software; Mediant 90xx.

2.8.1.6 Media Path Optimization in Media Bypass Mode for Direct Routing

The device now supports Microsoft's proprietary SIP header X-MS-UserSite, which is used for Local Media Optimization in Microsoft's Teams environments. This header, which is present in the SIP message received from the Teams client, indicates the Teams site (name) within which the Teams client is located. Based on this header, the device can now determine if the path (connectivity) between the Teams clients is good for voice quality and thus, intended for direct media calls.

The following configuration has been updated due to this support:

- The device's handling of Teams calls to determine direct media has been updated regarding the existing IP Group's 'Teams Local Media Optimization Handling' parameter. For more information, refer to the *User's Manual*.
- For determining if the path is good for voice quality and thus, intended for direct media, the device uses the following mechanism:
  - A new parameter 'Teams Local Media Optimization Site' has been added to the IP Groups table to define the name of the Teams site (e.g., "Singapore"). For each IP Group representing specific Teams clients, this parameter is configured accordingly with the site's name.

  - A Dial Plan is used to determine if the path between the Teams clients is intended for direct media. The Dial Plan is specified by the new parameter 'Region Connectivity Dial Plan'. Each Dial Plan rule in the Dial Plan is configured with a Teams site name in the 'Prefix' parameter (e.g., "Singapore") and with logical group(s) to which the Teams site belongs in the 'Tag' parameter (e.g., "Group=2,7"). When the device receives the SIP dialog from a Teams client, it checks the Dial Plan to see if the Teams sites of the source and destination Teams clients share a common group number. If they do, the device considers the call as direct media.

Applicable Application: SBC.

Applicable Products: All.

2.8.1.7 Bulk Software Upgrade of Media Cluster Via OVOC

OVOC can now be used to upgrade a media cluster (multiple Media Components or also referred to as MTs) for the Media Transcoding Cluster (MTC) feature or Elastic Media Cluster feature (Mediant CE). During the upgrade, the Signaling Component (SC) sends status updates of the upgrade process to OVOC.

Applicable Application: SBC.

Applicable Products: Mediant 90xx (with MTs); Mediant CE; Mediant VE.

2.8.1.8 TLS Context (Certificate) Enhancements

TLS Context (certificate) configuration includes the following enhancements:

- A device reset is no longer required when adding or modifying TLS Context parameters, including their related files (self-signed certificates, private keys or root certificates).
- Private key size of 1024 is no longer an optional value.
- SHA-1 has been removed as an optional value for the signature algorithm.
- CLI commands have been restructured.
- The Change Certificates page (child of the TLS Contexts page) in the Web interface has been updated with regards to design.

Applicable Application: All.

Applicable Products: All.

2.8.1.9 CNAME and SRV DNS Queries for Firewall

The device's firewall (access list), which is configured in the Firewall table, now supports CNAME and SRV DNS queries when the 'Source IP' parameter is configured with an FQDN.

A CNAME query for an FQDN replies with the canonical name of the requested FQDN. This hostname is used to resolve the IP address. An SRV query for an FQDN replies with a service list of one or more SRV records, each containing multiple fields, including the canonical hostname of the machine providing the service. This hostname is used to resolve the IP address. Up until now, if an FQDN was configured, the device performed an A-record DNS query to resolve the domain name into an IPv4 IP address.

The feature is supported by a new parameter in the Firewall table, 'DNS Query Type' (DnsQueryType) which allows the user to choose the DNS query type:

- [1] A (default and for IPv4 queries)
- [2] AAAA (IPv6 queries)
- [3] CNAME A (cname query, resolved into IPv4 address)
- [4] CNAME AAAA (cname query, resolved into an IPv6 address)
- [5] SRV A (SRV query, resolved into an IPv4 address)

- [6] SRV AAAA (SRV query, resolved into an IPv6 address)

The device performs DNS resolution periodically (i.e., resolved addresses are not persistent).

For the CLI command `nslookup`, support for SRV/CNAME resolution types has also been added:

```
nslookup <hostname> [source voip interface vlan] type
<A/AAAA/SRV/CNAME>
```

A total of 500 IP addresses can be added to the Firewall (defined as IP addresses or resolved by DNS).

Applicable Application: All.

Applicable Products: All.

2.8.1.10 Persistent Logging

The device now automatically saves logged event messages on its local storage memory, which remain (persistent) even after the device resets or powers off. This functionality is by default and can't be disabled.

- The device can store up to 10 persistent log files. The maximum size (in KB) of each file (default is 1,024 KB) can be configured by the new parameter SystemPersistentLogSize (`configure troubleshoot > syslog > system-persistent-log-size`).
- Persistent log file contents can be viewed using the new CLI command `show system log persistent`.

  (The `show system persistent-log` and `debug persistent-log` commands are now obsolete.)
- Persistent log files can be downloaded or sent to a remote server, using the new CLI command `copy system-log-persistent to`.

Note: This feature replaces the persistent logging feature supported by Mediant 90xx and Mediant Software in Version 7.2.

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.8.1.11 Enhanced Logging Features

The following enhancements have been made to the logging feature:

- Viewing logs through the CLI can be filtered to include only non-SIP logged messages, using the new CLI command `show system log no-sip`.
- Downloading logged files (compressed in tar.gz format):
  - `copy system-log to`: downloads system log file
  - `copy system-log-no-sip to`: downloads system log file without SIP-related information
- The debug file (`show debug-file`) now also includes persistent logs, no-sip logs, and syslog of kernel

- A new SNMP trap event is sent when debug recording is activated (acDebugRecordingActivationAlarm / OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.150)

Applicable Application: All.

Applicable Products: All.

2.8.1.12 AudioCodes Plugins No Longer Required for Wireshark

Installing AudioCodes Wireshark packet-dissector plugins are no longer required from Wireshark Version 3.4.0 and later. The plugins have now been integrated into the Wireshark open-source application, providing built-in support for AudioCodes Debug Recording (ACDR).

Applicable Application: All.

Applicable Products: All.

2.8.1.13 CAC Algorithm Based on Sliding Window Counter

The device's Call Admission Control (CAC) now supports an additional, more accurate rate-limiting algorithm for SIP dialogs based on a *sliding window counter*, than the already supported token bucket algorithm.

The Sliding Window counter algorithm sets a rate for the window, where the window is the previous (last) second to when the incoming SIP dialog-initiating request (e.g., INVITE) is received. When the device receives a new SIP dialog request, it checks how many dialog requests were received in the window (previous second). If the number (counter) is below the configured rate, the device accepts the SIP dialog. If the number is at the configured rate, the device rejects the call.

For example, assume the rate is configured to 5. If the device receives a new incoming SIP-dialog request at 18:00:01 (hh:mm:ss) and only 4 dialog requests were received in the previous window (i.e., 18:00:00-18:00:01), it accepts the new dialog request. However, if 5 dialog requests were received in the window when the new dialog arrived, the new dialog is rejected.

This new CAC algorithm is enabled (disabled by default) by the new parameter 'Sliding Window Counter Rate Limiting Algorithm For CAC'.

In addition to this feature, the following existing parameters now have a valid value range (0-65535): 'Rate', 'Rate Per User', 'Maximum Burst', 'Maximum Burst Per User'. Note that if configured out of this range in a previous version when upgrading to Version 7.4, if the value is less than 0 the value is set to 0 and if the value is greater than 65,535 it is set to 65,535.

Applicable Application: SBC.

Applicable Products: Mediant 90xx, Mediant Software.

2.8.1.14 Debug Recording Enhancements

The device's debug recording feature has been enhanced:

- Logging Filters table:
  - (Only Mediant 90xx and Mediant Software) Up until now, local storage ('Log Destination' set to **Local Storage**) was supported only for CDRs ('Log Type' set to **CDR Only**). Now, local storage is also supported for the following log types:
    - Signaling
    - Signaling & Media
    - Signaling & Media & PCM
    - SIP Only

  - New 'Filter Type' value called **System Trace**, which includes logs that don't relate to calls (e.g., CPU or disconnected LDAP server; HA traffic between active and redundant). When selected, the 'Value' parameter can be configured to one of the following values:
    - "syslog": INFO packets
    - "tpncp": device event and command packets as shown when using "tpncp" Wireshark filter
    - "ha": communication between active and redundant
- A new page titled "Debug Recording" has been added (Troubleshoot menu > Troubleshoot tab > Logging folder > Debug Recording), which contains the following groups of parameters:
  - **IP Trace:** This group provides new parameters for filtering IP traces when the Logging Filters table has a rule whose 'Filter Type' parameter is set to **IP Trace**. The traces can be filtered by a specific physical entity -- Ethernet port, VLAN, or Ethernet Group (Mediant 90xx and Mediant Software only). If not specified (default), the IP trace records traffic received from and transmitted to all ports.
  - **Debug Recording Server:** The debug recording parameters under this group were moved from the Debug Recording group on the existing Logging Settings page ('Debug Recording Destination IP', 'Debug Recording Destination Port' and 'Debug Recording Interface Name'). In addition, "Debug Recording" has been removed from their parameter names.
  - **Local Files Storage:** (Only Mediant 90xx and Mediant Software) Local storage of debug recording files are now supported. This is relevant for Logging Filter rules whose 'Log Destination' parameter is configured to **Local Storage** and 'Log Types' configured to any value except **CDR Only** or **Call Flow**. New parameters have been added to support the feature - 'Local Storage', 'Recording', 'File Size', 'Number of Files', 'File Mode' and 'Rotation Period'
- SFTP can be used to download locally stored debug files.
- Up until now, after an HA switchover, only data was recorded (not media/RTP) for IP traces. Now, the IP trace also includes media after a switchover.

Applicable Application: All.

Applicable Products: All.

2.8.1.15 Maximum Characters Increased for Dial Plan Tags

The maximum number of characters that can be configured for Dial Plan tags in the Dial Plan Rule table ('Tag' parameter) has been increased from 120 to 255.

Applicable Application: SBC.

Applicable Products: Mediant 90xx; Mediant Software.

2.8.1.16 Maximum IP Profiles Increased

The maximum number of IP Profiles that can be configured (in the IP Profiles table) has been increased to 1,500 for devices supporting 64 GB storage.

Applicable Application: SBC.

Applicable Products: Mediant VE/CE.

2.8.1.17 Interworking between ISDN CUG and SIP

The device now supports interworking between the ISDN Closed User Group (CUG) supplementary service and SIP, for Tel-to-IP calls. The CUG supplementary service enables users to form groups, where members of a specific closed user group can communicate among themselves but not, in general, with users outside the group.

If this feature is enabled and the device receives an ISDN Setup message whose Facility IE indicates CUG (cUGCall invoke), it adds an XML body containing CUG information (CUG index and outgoing access) to the outgoing SIP INVITE message, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
targetNamespace="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xs:annotation>
<xs:documentation>XML Schema definition for the closed user group
parameter</xs:documentation>
</xs:annotation>
<xs:include schemaLocation="xcap.xsd"/>
<!--Definition of simple types-->
<xs:simpleType name="twobitType">
<xs:restriction base="xs:string">
<xs:pattern value="[0-1][0-1]"/>
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="networkIdentityType">
<xs:restriction base="xs:hexBinary">
<xs:length value="2"/>
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="sixteenbitType">
<xs:restriction base="xs:hexBinary">
<xs:length value="2"/>
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="cugIndexType">
<xs:restriction base="xs:integer">
<xs:minInclusive value="0"/>
<xs:maxInclusive value="32767"/>
</xs:restriction>
</xs:simpleType>
<!--Definition of complex types-->
<xs:complexType name="cugRequestType">
<xs:sequence>
<xs:element name="outgoingAccessRequest" type="xs:boolean"/>
<xs:element name="cugIndex" type="cugIndexType" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<!--Definition of document structure-->
<xs:element name="cug" substitutionGroup="ss:ssbsService">
<xs:complexType>
<xs:complexContent>
<xs:extension base="ss:simservType">
<xs:sequence>
<xs:element name="cugCallOperation" type="cugRequestType"
minOccurs="0">
</xs:complexType>
```

S6

```
<xs:sequence>
<xs:element name="outgoingAccessRequest" type="xs:boolean"
value="true"/>
<xs:element name="cugIndex" type="xs:integer" value="32767"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="networkIndicator" type="networkIdentityType"
minOccurs="0"/>
<xs:element name="cugInterlockBinaryCode" type="sixteenbitType"
minOccurs="0"/>
<xs:element name="cugCommunicationIndicator" type="twobitType"
minOccurs="0"/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:element>
</xs:schema>
```

The feature is enabled by the new parameter, 'Cug Data Mode' (CugDataMode / cug-data-mode). By default (disabled), the device doesn't add the CUG body. If enabled, the device adds the CUG XML body.

Applicable Application: Gateway (ISDN).

Applicable Products: Mediant 500; Mediant 800; Mediant 1000.

2.8.1.18 Activity Log Includes Parameter Changes from Incremental ini File

The existing Activity Log, which sends logs of selected management user operations done in the device's management interfaces to Syslog, can now be enabled to include a log of parameter changes due to an uploaded incremental ini file. When loading an incremental ini file, only parameter settings included in the ini file are applied to the device; all other parameters remain at their current settings. This feature applies to incremental ini file load through the Web interface (Auxiliary Files page) or CLI (`copy incremental-ini-file from`).

The feature is enabled by a new checkbox located under the Activity Log group in the Web interface (`configure troubleshoot > activity-log > incremental-ini-log`). In addition, the maximum number of lines (not empty or comments) to log from the ini file can be configured using the new parameter MaxINIActivityLog (`configure troubleshoot > max-ini-activity-logs`).

Applicable Application: All.

Applicable Products: All.

2.8.1.19 NGINX Syntactic Errors Displayed in Syslog

Syntactic errors when adding NGINX directives (in the HTTP Directive Sets > HTTP Directives table) for the device's HTTP Proxy functionality are now reflected in Syslog messages. Up until now, they were displayed only in the device's CLI (`show network http-proxy conf errors`).

Applicable Application: SBC.

Applicable Products: All.

2.8.1.20 Incremental ini File Load through SNMP

SNMP can now be used to load an incremental ini file to the device from a remote HTTP-based server. This is done using the new MIB object, acSysHTTPClientIncrementalIniFileURL. The corresponding existing ini file parameter is IncrementalIniFileURL.

Applicable Application: All.

Applicable Products: All.

2.8.1.21 B-Channel Negotiation Mode Configuration Update

As the CLI command `b-ch-negotiation` is a global parameter (i.e., affecting all trunks), it has been moved from `configure voip > interface el-t1|b1` to `configure voip > gateway digital settings`. A new CLI command, `b-channel-nego-per-trunk` has been added to `configure voip > interface el-t1|b1` for configuring B-channel negotiation mode per trunk.

Applicable Application: Gateway (Digital).

Applicable Products: Digital.

2.8.1.22 Maximum Stored Historical SBC CDRs Reduced

The maximum number of historical SBC CDRs that can be stored on the device (and displayed in the SBC CDR History table) has been reduced for some products, as follows:

- 2,048 (instead of 4,096): MP-1288, Mediant 500, Mediant 500L, Mediant 800 and Mediant 1000
- 4,096: Mediant 2600 and Mediant 4000

Applicable Application: SBC.

Applicable Products: MP-1288; Mediant 500; Mediant 500L; Mediant 800; Mediant 1000; Mediant 2600; Mediant 4000.

2.8.1.23 Management User Password Hidden in Activity Log

When password obscurity is enabled or enforced (`obscure-password-mode on` and `enforce-password-complexity`) and a password is configured for a new management user (successfully or not) or the password of an existing user is modified (Local Users table), if reporting of management user activities is enabled, the password is not shown in the Activity Log.

Applicable Application: All.

Applicable Products: All.

2.8.1.24 Reduction in Excess SIP Interfaces

As the maximum number of SIP Interfaces was more than required for typical deployments, the maximum has been reduced to free-up memory for other functionality.

- MP-1288, Mediant 500/L, Mediant 800, Mediant 1000: 80 (was 82)
- Mediant 2600, Mediant 4000: 700 (was 1,200)
- Mediant 90xx: 1,200 (no change)
- Mediant Software:
  - 2 GB: 40 (was 600)
  - 3 GB: 200 (was 1,200)
  - 4 GB: 400 (was 1,200)
  - 8 GB: 800 (was 1,200)
  - 16 GB: 1,200 (no change)
  - 32-64 GB: 1,200 (no change)

Note: When upgrading to Version 7.4 from an earlier version when the device is configured with more SIP Interfaces than the new maximum number of allowed SIP Interfaces for Ver. 7.4, the excess configured SIP Interfaces (trimmed from the SIP Interface with the highest table row index) are deleted. For example, if there are 1,000 SIP Interfaces in Ver. 7.2, only the first 700 SIP Interfaces in the table remain after the upgrade to Ver. 7.4.

Applicable Application: All.

Applicable Products: All.

2.8.1.25 New Hardware Revision for CRMX Module

The CRMX module, which is housed in the Mediant 1000 E-SBC & Gateway, was updated due to one of its components reaching End-Of-Life (EOL) status. The new CRMX module no longer has a WAN port (which was not used and covered by a metal plate).

The new CRMX module is compatible with Software Version 7.40A.002.007 and later.

Applicable Application: All.

Applicable Products: Mediant 1000.

2.8.2 Known Constraints

This section lists known constraints.

Table 2-11: Known Constraints in Version 7.4

Incident	Description
-	The following products are not supported in this version: • Mediant 9000 SBC • Mediant 9030 SBC • Mediant 9080 SBC • Mediant SE SBC • Mediant VE SBC • Mediant CE SBC
SBC-24381	For the Lawful Interception feature, the target's XID can only be configured to a numerical value. If it's alphanumeric, it can't be deleted nor updated.

2.8.3 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 2-12: Resolved Constraints in Version 7.4

Incident	Description
SBC-15662	The device experiences no audio after an attempt to replace the TLS certificate on the fly (without a reset). **Applicable Products:** All
SBC-16401	The device generates the following messages to the CLI: "file truncated /sbin/tail: /var/log/messages:" and "/sbin/tail: /var/log/messages: file truncated". **Applicable Products:** All
SBC-16408	Customizing user-level access privileges for Web interface pages doesn't apply to the import and export commands of the Action button on Web pages that provide this button. For example, if the Malicious Signature table is customized to read-write for all users, it doesn't apply this to the import/export actions (and only Security Admin can import/export). **Applicable Products:** All
SBC-17014	The value of the performance monitoring parameter for attempted calls count doesn't match the CDR. **Applicable Products:** All
SBC-17618	Device's Web interface is using outdated libraries. These libraries have now been updated.
SBC-18658	The associated contact address (AOR) is not updated in the database after changes in the Dial Plan. **Applicable Products:** All
SBC-19202	The device is exposed to a security vulnerability, allowing HTML injection tags/scripts to search a term. **Applicable Products:** All
SBC-19603 / SBC-21622	Lines (rows) in the Classification table of the Web interface cannot be reordered. **Applicable Products:** All
SBC-20216	The CLI `ping` command doesn't function for IPv4 addresses. **Applicable Products:** All
SBC-21716	Filtering the `show voip calls` command output using the grep filter (`| grep`) doesn't function. This has been resolved by replacing the grep switch with the new `match` switch, which provides a simple string match of the call detail record text. For example, to search the string "abc": `show voip calls active abc match abc` **Applicable Products:** All
SBC-21801	Loading an ini file to the SBC through OVOC doesn't function properly when SetDefaultOnIniFileProcess parameter is configured to 0. **Applicable Products:** All

3 Session Capacity

This section provides capacity for the Gateway and SBC products.

3.1 SIP Signaling and Media Capacity

The following table lists the maximum, concurrent SIP signaling sessions, concurrent media sessions, and registered users per product.

Table 3-1: SIP Signaling and Media Capacity per Product

Product		Signaling Capacity		Media Sessions			
		SIP Sessions	Registered Users	Session Type	RTP	SRTP	Detailed Media Capabilities
Mediant 500		250	1,500	Hybrid	250	200	Transcoding: n/a GW: Table 3-4
				GW-Only	30	30	
Mediant 500L		60	200	Hybrid	60	60	Transcoding: n/a GW: Table 3-6
				GW-Only	8	8	
Mediant 800B		250	1,500	Hybrid	250	250	GW & Transcoding: Table 3-8 SBC Only: Table 3-7
				GW-Only	64	64	
Mediant 800C		400	2,000	Hybrid	400	300	GW & Transcoding: Table 3-10
				GW-Only	124	124	
Mediant 1000B		150	600	Hybrid	150	120	Transcoding: Table 3-14 GW: Tables Table 3-11, Table 3-12, Table 3-13
				GW-Only	192	140	
MP-1288		588	350	Hybrid	588	438	Transcoding: n/a GW: Table 3-15
				SBC-Only	300	300	
				GW-Only	288	288	
Mediant 2600		600	8,000	SBC-Only	600	600	Transcoding: Table 3-16
Mediant 4000		5,000	20,000	SBC-Only	5,000	3,000	Transcoding: Table 3-17
Mediant 4000B		5,000	20,000	SBC-Only	5,000	5,000	Transcoding: Table 3-19
Mediant 9000	SIP Performance Profile (HT Enabled)	30,000	300,000	SBC-Only	30,000	16,000	Transcoding: n/a
		55,000	0	SBC-Only	55,000	18,000	Transcoding: n/a
	DSP Performance Profile (HT Enabled)	50,000	0	SBC-Only	50,000	18,000	Transcoding: Table 3-21
	SRTP Performance Profile (HT Enabled)	50,000	0	SBC-Only	50,000	40,000	Transcoding: n/a
Mediant 9000	SIP Performance Profile	50,000	500,000	SBC-Only	50,000	30,000	Transcoding: n/a
		70,000	0	SBC-Only	70,000	30,000	Transcoding: n/a
	DSP Performance Profile	50,000	0	SBC-Only	50,000	28,000	Transcoding: Table 3-23
	SRTP Performance Profile	70,000	0	SBC-Only	70,000	40,000	Transcoding: n/a
Mediant 9030	SIP Performance Profile	30,000	200,000	SBC-Only	30,000	30,000	Transcoding: n/a
	DSP Performance Profile	30,000	200,000	SBC-Only	30,000	15,000	Transcoding: Table 3-26
Mediant 9080	SIP Performance Profile	50,000	500,000	SBC-Only	50,000	30,000	Transcoding: n/a
		70,000	0	SBC-Only	70,000	30,000	Transcoding: n/a
	DSP Performance Profile	50,000	0	SBC-Only	50,000	28,000	Transcoding: Table 3-23
	SRTP Performance Profile	70,000	0	SBC-Only	70,000	40,000	Transcoding: n/a
Mediant 9000 with Media Transcoders (MT-type)		24,000	180,000	SBC-Only	24,000	16,000	Transcoding: Table 3-25

Product			Signaling Capacity		Media Sessions			
			SIP Sessions	Registered Users	Session Type	RTP	SRTP	Detailed Media Capabilities
Mediant 9000 Rev. B with Media Transcoders (MT-type)			60,000	200,000	SBC-Only	60,000	40,000	Transcoding: Table 3-25
Mediant 9080 with Media Transcoders (MT-type)			60,000	200,000	SBC-Only	60,000	40,000	Transcoding: Table 3-25
Mediant CE	AWS / EC2		50,000	100,000	SBC-Only	50,000	50,000	Forwarding: Table 3-28 Transcoding: Table 3-29
	Azure		36,000	75,000	SBC-Only	36,000	32,000	Forwarding: Table 3-30
			32,000	75,000	SBC-Only	32,000	32,000	Forwarding: Table 3-30 Transcoding: Table 3-31
	VMware		12,000	100,000	SBC-Only	12,000	12,000	Forwarding: Table 3-32 Transcoding: Table 3-33
Mediant VE	VMware	1 vCPU 2-GB RAM (HT)	250	1,000	SBC-Only	250	250	Transcoding: n/a
		1 vCPU 8-GB RAM (HT)	4000	15,000	SBC-Only	4000	2600	Transcoding: n/a
		4 vCPU 16-GB RAM (HT)	8,000	75,000	SBC-Only	8,000	6,000	Transcoding: n/a
		2 vCPUs 8-GB RAM (HT)	4000	15000	SBC-Only	2200	1900	Transcoding: Table 3-34
		4 vCPU 8-GB RAM (HT)	4,000	15,000	SBC-Only	1,800	1600	Transcoding: Table 3-34
		8 vCPU 16-GB RAM (HT)	9,000	75,000	SBC-Only	6,000	5,000	Transcoding: Table 3-34
		16 vCPU 16-GB RAM (HT)	9,000	75,000	SBC-Only	6,500	5,000	Transcoding: Table 3-34
	KVM/OpenStack	1 vCPU 2-GB RAM (HT)	250	1,000	SBC-Only	250	250	Transcoding: n/a
		1 vCPU 8-GB RAM (HT)	2,500	15,000	SBC-Only	2,500	1,700	Transcoding: n/a
		4 vCPU 16-GB RAM (HT)	4,500	75,000	SBC-Only	4,500	3,500	Transcoding: n/a
		2 vCPUs 8-GB RAM (HT)	1,900	15,000	SBC-Only	1,900	1,400	Transcoding: Table 3-34
		8 vCPU 16-GB RAM (HT)	5,800	75,000	SBC-Only	5,800	4,800	Transcoding: Table 3-34
		16 vCPU 16-GB RAM (HT)	3,800	75,000	SBC-Only	3,800	2,800	Transcoding: Table 3-34
		8 vCPU 32-GB RAM SR-IOV Intel NICs (non-HT)	24,000	75,000	SBC-Only	24,000	10,000	Transcoding: n/a
	Hyper-V	1 vCPU 2-GB RAM (HT)	250	1,000	SBC-Only	250	250	Transcoding: n/a
		1 vCPU 8-GB RAM (HT)	1,500	15,000	SBC-Only	1,500	1,200	Transcoding: n/a
		4 vCPU 8-GB RAM (HT)	2,500	75,000	SBC-Only	2,500	2,300	Transcoding: n/a
		2 vCPUs 8-GB RAM (HT)	1,900	15,000	SBC-Only	1,900	1,400	Transcoding: Table 3-34

Product			Signaling Capacity		Media Sessions			
			SIP Sessions	Registered Users	Session Type	RTP	SRTP	Detailed Media Capabilities
Mediant SE	AWS / EC2	8 vCPU 16-GB RAM (HT)	2,500	75,000	SBC-Only	2,500	2,300	Transcoding: Table 3-34
		m5.large	6,000	75,000	SBC-Only	6,000	5,500	Transcoding: n/a
		c5.2xlarge	5,500	75,000	SBC-Only	5,500	5,000	Transcoding: Table 3-35
		c5.9xlarge	7,000	75,000	SBC-Only	7,000	6,000	Transcoding: Table 3-36
	Azure	DS1_v2	600	1,000	SBC-Only	600	500	Transcoding: n/a
			300	1,000	SBC-Only	300	300	Transcoding: Table 3-38
		DS2_v2	1,200	15,000	SBC-Only	1,200	800	Transcoding: n/a
			900	15,000	SBC-Only	900	600	Transcoding: Table 3-38
		DS3_v2	1,700	50,000	SBC-Only	1,700	1,600	Transcoding: n/a
			1,100	50,000	SBC-Only	1,100	800	Transcoding: Table 3-38
		DS4_v2	1,800	75,000	SBC-Only	1,800	1,600	Transcoding: n/a
			1,600	75,000	SBC-Only	1,600	1,600	Transcoding: Table 3-38
	DL380p Gen8 or DL360 Gen9		24,000	120,000	SBC-Only	16,000	14,000	Transcoding: n/a
			24,000	0	SBC-Only	24,000	14,000	Transcoding: n/a
	DL380 Gen10	SIP Performance Profile	50,000	500,000	SBC-Only	50,000	30,000	Transcoding: n/a
			70,000	0	SBC-Only	70,000	30,000	Transcoding: n/a
		DSP Performance Profile	50,000	0	SBC-Only	50,000	28,000	Transcoding: Table 3-39
		SRTP Performance Profile	70,000	0	SBC-Only	70,000	40,000	Transcoding: n/a

Notes:

- The figures listed in the table are accurate at the time of publication of this document. However, these figures may change due to a later software update. For the latest figures, please contact your AudioCodes sales representative.
- "GW" refers to Gateway functionality.
- "SIP Sessions" refers to the maximum concurrent signaling sessions for both SBC and Gateway (when applicable). Whenever signaling sessions is above the maximum media sessions, the rest of the signaling sessions can be used for Direct Media.
- "Session Type" refers to Gateway-only sessions, SBC-only sessions, or Hybrid sessions which is any mixture of SBC and Gateway sessions under the limitations of Gateway-only or SBC-only maximum values.
- "RTP Sessions" refers to the maximum concurrent RTP sessions when all sessions are RTP-RTP (for SBC sessions) or TDM-RTP (for Gateway sessions).
- "SRTP Sessions" refers to the maximum concurrent SRTP sessions when all sessions are RTP-SRTP (for SBC sessions) or TDM-SRTP (for Gateway sessions).
- "Registered Users" refers to the maximum number of users that can be registered with the device. This applies to the supported application (SBC or CRP).

- Regarding signaling, media, and transcoding session resources:
  - A signaling session is a SIP dialog session between two SIP entities, traversing the SBC and using one signaling session resource.
  - A media session is an audio (RTP or SRTP), fax (T.38), or video session between two SIP entities, traversing the SBC and using one media session resource.
  - A gateway session (i.e. TDM-RTP or TDM-SRTP) is also considered as a media session for the calculation of media sessions. In other words, the maximum Media Sessions specified in the table refer to the sum of Gateway and SBC sessions.
  - In case of direct media (i.e., Anti-tromboning / Non-Media Anchoring), where only SIP signaling traverses the SBC and media flows directly between the SIP entities, only a signaling session resource is used. Thus, for products with a greater signaling session capacity than media, even when media session resources have been exhausted, additional signaling sessions can still be handled for direct-media calls.
  - For call sessions requiring transcoding, one transcoding session resource is also used. For example, for a non-direct media call in which one leg uses G.711 and the other leg G.729, one signaling resource, one media session resource, and one transcoding session resource is used.
- Capacity of the Cloud Resilience Package (CRP) application is listed under "Registered Users".
- Capacity of the Lync Analog Device (LAD) application is listed under "Media Sessions".
- **MP-1288:** The maximum number of media and signaling sessions is the summation of the maximum 300 RTP-to-RTP (SBC) sessions and the maximum 288 TDM-RTP (Gateway) sessions. The maximum number of SRTP sessions is the summation of the maximum 150 RTP-to-SRTP (SBC) sessions and the maximum 288 TDM-SRTP (Gateway) sessions.
- Media Transcoding Cluster (MTC) feature is not supported by Mediant 9030 SBC.
- **Mediant 90xx SBC with Media Transcoders limitations:**
  * To allow DSP capabilities (such as transcoding), the Performance Profile parameter must be configured to the DSP profile.
  Each transcoding session is weighted as two RTP-RTP sessions without transcoding. Therefore, the number of sessions without transcoding plus the doubled number of sessions with transcoding must be less than the maximum RTP-RTP figure specified in the table. As result, if all sessions involve transcoding, the maximum number of sessions is half the maximum RTP-RTP sessions without transcoding specified in the table.
  ** The maximum SRTP-RTP sessions is also effected by the above limitations. For example, if sessions involve transcoding, the maximum number of SRTP-RTP sessions is also limited by half of the maximum SRTP-RTP sessions without transcoding.
- **Mediant VE SBC for VMware:** The profiles are applicable to when ESXi version is 6.7 or later, host's CPU is Intel Xeon Scalable Processors, and Hyper-Threading is enabled. For example, a 4-vCPU virtual machine allocates only 2 physical cores. For minimum requirements, see Section 3.3.14.1 on page 84.
- **Mediant CE:** Based on the following instances:
  - AWS:
    - Signaling Components (SC): m5.2xlarge
    - Media Components (MC) - forwarding only: m5.large
    - MC - forwarding and transcoding: c5.4xlarge
  - Azure:
    - SC: DS3_v2 (up to 50K users) or D8s_v3/v4 (up to 75K users)
    - MC - forwarding only: DS2_v2, DS3_v2 or DS4_v2

- MC - forwarding and transcoding: DS2_v2, DS3_v2, or DS4_v2
- VMware:
  - SC: 8-vCPU (Hyper-Threaded), 16-GB RAM
  - MC - forwarding only: 2-vCPU (Hyper-Threaded), 8-GB RAM
  - MC - forwarding and transcoding: 8-vCPU (Hyper-Threaded), 8-GB RAM
- **Mediant SE:** For new deployments, it's highly recommended to use the DL360 G10 server. For exact specifications and BIOS settings, please contact your AudioCodes sales representative.

3.2 Capacity per Feature

The table below lists capacity per feature.

Table 3-2: Capacity per Feature

Product	Max. Concurrent WebRTC Sessions (see Note #3)		Max. One-Voice Resiliency (OVR) Users	Max. Concurrent SIPRec Sessions (see Note #4)
	Click-to-Call	Registered Agents		
MP-1288	-	-	-	150
Mediant 500	-	-	-	125
Mediant 500L	-	-	-	30
Mediant 800B	100	100	100	200
Mediant 800C	100	100	150	200
Mediant 1000B	-	-	50	-
Mediant 2600	600	600	-	300
Mediant 4000B / Mediant 4000	1,000	1,000	-	2,500
Mediant 9000	5,000	16,000	-	• With Hyper-Threading: 20,000 • Without Hyper-Threading: 12,000
Mediant 9030	5,000	16,000	-	15,000
Mediant 9080	8,000	25,000	-	20,000
Mediant SE (see Note #1)	5,000	25,000	-	12,000
Mediant VE (see Note #2)	5,000	5,000	2,000	12,000
Mediant CE (see Note #2)	5,000	5,000	-	20,000

Note:

1. Using the approved SE server specifications with an Intel Xeon Gold 6126 processor. For the specifications, please contact AudioCodes.
2. The maximum number of WebRTC sessions cannot be higher than the number of SRTP sessions, as indicated in Table 3-1. Therefore, the actual maximum number of concurrent WebRTC sessions per deployment environment will be the lower of these numbers.
3. The capacity figures assume that a TLS key size of 2048-bit is used for the WebSocket and DTLS negotiation.
4. The capacity figures for SIPRec assume that there are no other concurrent, regular (non-SIPRec) voice sessions. SIPRec sessions are counted as part of the SBC session capacity. The maximum number of SIPRec sessions cannot be higher than the number of RTP sessions, as indicated in Table 3-1. Therefore, the actual maximum number of SIPRec sessions per deployment environment will be the lower of these numbers.

3.3 Detailed Capacity

This section provides detailed capacity figures.

3.3.1 Mediant 500 E-SBC

The SBC session capacity and DSP channel capacity for Mediant 500 E-SBC are shown in the tables below.

3.3.1.1 Non-Hybrid (SBC) Capacity

Table 3-3: Mediant 500 E-SBC (Non-Hybrid) - SBC Capacity

Hardware Configuration	TDM-RTP Sessions				Max. SBC Sessions (RTP-RTP)
	DSP Channels Allocated for PSTN	Wideband Coders			
		G.722	AMR-WB (G.722.2)	SILK-WB	
SBC	n/a	n/a	n/a	n/a	250

3.3.1.2 Hybrid (with Gateway) Capacity

Table 3-4: Mediant 500 Hybrid E-SBC (with Gateway) - Media & SBC Capacity

Hardware Configuration	TDM-RTP Sessions				Max. SBC Sessions (RTP-RTP)
	DSP Channels Allocated for PSTN	Wideband Coders			
		G.722	AMR-WB (G.722.2)	SILK-WB	
1 x E1/T1	30/24	√	-	-	220/226
	26/24	√	√	-	224/226
	26/24	√	√	√	224/226

3.3.2 Mediant 500L Gateway and E-SBC

The SBC session capacity and DSP channel capacity for Mediant 500L Gateway and E-SBC is shown in the tables below.

3.3.2.1 Non-Hybrid (SBC) Capacity

Table 3-5: Mediant 500L E-SBC (Non-Hybrid) - SBC Capacity

Hardware Configuration	TDM-RTP Sessions			Max. SBC Sessions (RTP-RTP)
	DSP Channels Allocated for PSTN	Wideband Coders		
		G.722	AMR-WB (G.722.2)	
SBC	n/a	n/a	n/a	60

3.3.2.2 Hybrid (with Gateway) Capacity

Table 3-6: Mediant 500L Hybrid E-SBC (with Gateway) - Media & SBC Capacity

Hardware Configuration	DSP Channels Allocated for PSTN	Additional Coders				Max. SBC Sessions
		Narrowband	Wideband			
		Opus-NB	G.722	AMR-WB (G.722.2)	Opus-WB	
2 x BRI / 4 x BRI	4/8	-	-	-	-	56/52
	4/8	-	√	-	-	56/52
	4/6	√	-	√	-	56/54
	4	-	-	-	√	56

S9

3.3.3 Mediant 800 Gateway & E-SBC

This section describes capacity for Mediant 800 Gateway & E-SBC.

3.3.3.1 Mediant 800B Gateway & E-SBC

The DSP channel capacity and SBC session capacity for Mediant 800B Gateway & E-SBC are shown in the tables below.

3.3.3.1.1 Non-Hybrid (SBC) Capacity

Table 3-7: Mediant 800B Gateway & E-SBC - SBC Session Capacity per Capabilities (SBC Only)

H/W Configuration	DSP Channels for PSTN	SBC Transcoding Sessions								
		From Profile 2 with Additional Advanced DSP Capabilities						To Profile 1	To Profile 2	Max. SBC Sessions
		Opus-NB	Opus-WB	AMR-NB / G.722	AMR-WB (G.722.2)	SILK-NB / iLBC	SILK-WB			
SBC	n/a	-	-	-	-	-	-	57	48	250
	n/a	-	-	√	-	-	-	51	42	250
	n/a	-	-	-	-	√	-	39	33	250
	n/a	-	-	-	√	-	-	36	30	250
	n/a	-	-	-	-	-	√	27	24	250
	n/a	√	-	-	-	-	-	27	24	250
	n/a	-	√	-	-	-	-	21	21	250

Note: "Max. SBC Sessions" applies to scenarios without registered users. When registered users are used, "Max. SBC Sessions" is reduced according to the main capacity table (see Section 3.1).

3.3.3.1.2 Hybrid (with Gateway) Capacity

Table 3-8: Mediant 800B Gateway & E-SBC - Channel Capacity per Capabilities (with Gateway)

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions									Conf. Participants	Max. SBC Sessions
		From Profile 2 with Additional Advanced DSP Capabilities							To Profile 1	To Profile 2		
		AMR-NB / G.722	AMR-WB (G.722.2)	SILK-NB	SILK-WB	Opus-NB	Opus-WB	V.150.1				
2 x E1/T1	60/48	-	-	-	-	-	-	-	3/15	2/13	-	190/202
2 x T1	48	-	-	-	-	-	-	√	11	9	-	202
1 x E1/T1 8 x FXS/FXO	38/32	-	-	-	-	-	-	-	22/28	18/22	-	212/218
	38/32	-	-	√	-	-	-	-	8/12	7/11	-	212/218
1 x E1/T1	30/24	-	-	√	-	-		√	14/18	12/16	-	220/226
1 x E1 4 x BRI	38	-	-	-	-	-	-	-	22	18	-	212
1 x E1 4 x FXS	34	-	-	-	-	-	-	-	26	21	-	216
2 x E1 4 x FXS	64	-	-	-	-	-	-	-	0	0	-	186
4 x BRI 4 x FXS 4 x FXO	16	-	-	-	-	-	-	-	5	4	-	234
8 x BRI 4 x FXS	20	-	-	-	-	-	-	-	1	1	-	230
8 x BRI	16	-	-	-	-	-	-	-	5	4	-	234
12 x FXS	12	-	-	√	-	-	-	√	3	3	-	238
4 x FXS 8 x FXO	12	-	-	√	-	-	-	-	3	3	-	238
8 x FXS 4 x FXO	12	-	-	√	-	-	-	-	3	3	-	238
4 x BRI 4 x FXS	12	-	-	√	-	-	-	-	3	3	-	238
4 x FXS 4 x FXO	8	-	-	-	-	-	-	-	7	5	6	242
	8	-	-	√	-	-	-	-	6	6	-	242
4 x BRI	8	-	-	-	-	-	-	-	7	5	6	242
	8	-	-	√	-	-	-	-	6	6	-	242
1/2/3 x BRI	2/4/6	-	-	-	-	-	-	-	17/15 /14	14/13 /11	-	248/246/ 244

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions									Conf. Participants	Max. SBC Sessions
		From Profile 2 with Additional Advanced DSP Capabilities							To Profile 1	To Profile 2		
		AMR-NB / G.722	AMR-WB (G.722.2)	SILK-NB	SILK-WB	Opus-NB	Opus-WB	V.150.1				
4 x FXS or 4 x FXO	2/4/6	-	-	√	-	-	-	-	11/10 /8	10/8/ 7	-	248/246/ 244
	4	-	-	√	-	-	-	√	10	8	-	246
	4	√	-	-	-	-	-	-	12	10	4	246
	4	-	-	√	-	-	-	-	6	6	4	246
	4	-	√	√	-	-	-	-	4	4	4	246
	4	-	√	√	√	-	-	-	3	3	4	246
	4	-	-	-	-	√	-	-	1	0	4	246
	4	-	-	-	-	-	√	-	0	0	3	246
FXS, FXO, and/or BRI, but not in use	0	-	-	-	-	-	-	-	19	16	-	250

Notes:

- "Max. SBC Sessions" for Mediant 800B applies to scenarios without registered users. When registered users are used, "Max. SBC Sessions" is reduced according to the main capacity table (see Section 3.1).
- *Profile 1*: G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2*: G.711, G.726, G.729 (A / AB), and G.723.1, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- SBC enhancements (e.g. Acoustic Echo Suppressor, Noise Reduction) are also available for these configurations. For more information, please contact your AudioCodes sales representative.
- Automatic Gain Control (AGC) and Answer Detector / Answer Machine Detector (AD/AMD) are also available for these configurations. For more information, please contact your AudioCodes sales representative.
- V.150.1 is supported only for the US Department of Defense (DoD).
- *Transcoding Sessions* represents part of the total SBC sessions.
- Conference Participants represents the number of concurrent analog ports in a three-way conference call.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

3.3.3.2 Mediant 800C Gateway & E-SBC

The DSP channel capacity and SBC session capacity for Mediant 800C Gateway & E-SBC are shown in the tables below.

3.3.3.2.1 Non-Hybrid (SBC) Capacity

Table 3-9: Mediant 800C Gateway & E-SBC - SBC Session Capacity per Capabilities (SBC Only)

H/W Configuration	SBC Transcoding Sessions								
	From Profile 2 with Additional Advanced DSP Capabilities						To Profile 1	To Profile 2	Max. SBC Sessions
	Opus-NB	Opus-WB	AMR-NB / G.722	AMR-WB (G.722.2)	SILK-NB / iLBC	SILK-WB			
SBC	-	-	-	-	-	-	114	96	400
	-	-	√	-	-	-	102	84	400
	-	-	-	-	√	-	78	66	400
	-	-	-	√	-	-	72	60	400
	-	-	-	-	-	√	54	48	400
	√	-	-	-	-	-	54	48	400
	-	√	-	-	-	-	42	42	400

Note: "Max. SBC Sessions" applies to scenarios without registered users. When registered users are used, "Max. SBC Sessions" is reduced according to the main capacity table (see Section 3.1).

3.3.3.2.2 Hybrid (with Gateway) Capacity

Table 3-10: Mediant 800C Gateway & E-SBC - SBC Session Capacity per Capabilities with Gateway

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions								Max SBC Sessions
		From Profile 2	From Profile 2 with SILK-NB / iLBC	From Profile 2 with SILK-WB	From Profile 2 with OPUS-NB	From Profile 2 with OPUS-WB	From Profile 2 with Profile 2	To Profile 1	To Profile 2	
4 x E1/T1 4 x FXS	124/100	√	-	-	-	-	-	2/23	2/18	276/300
	102/100	-	√	-	-	-	-	0	0	298/300
	78	-	-	√	-	-	-	0	0	322
	72	-	-	-	√	-	-	0	0	328
	54	-	-	-	-	√	-	0	0	346
1 x E1/T1 4 x FXS	35/29	√	-	-	-	-	-	25/30	2025	365/371
	35/29	-	√	-	-	-	-	10/15	9/13	365/371
	35/29	-	-	√	-	-	-	1/5	1/5	365/371
	35/29	-	-	-	√	-	-	0/4	0/3	365/371
	27	-	-	-	-	√	-	0	0	373
8 x BRI 4 x FXS	20	√	-	-	-	-	-	38	31	380
	20	-	√	-	-	-	-	22	19	380
	20	-	-	√	-	-	-	12	11	380
	20	-	-	-	√	-	-	11	9	380
	20	-	-	-	-	√	-	4	3	380
Not in use	-	√	-	-	-	-	-	114	96	400
	-	-	√	-	-	-	-	78	66	400
	-	-	-	√	-	-	-	54	48	400
	-	-	-	-	√	-	-	54	48	400
	-	-	-	-	-	√	-	42	42	400

Notes:

- "Max. SBC Sessions" applies to scenarios without registered users. When registered users are used, "Max. SBC Sessions" is reduced according to the main capacity table (see Section 3.1).
- *Profile 1*: G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2*: G.711, G.726, G.729 (A / AB), and G.723.1, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- SBC enhancements (e.g. Acoustic Echo Suppressor, Noise Reduction) are also available for these configurations. For more information, please contact your AudioCodes sales representative.
- Automatic Gain Control (AGC) and Answer Detector / Answer Machine Detector (AD/AMD) are also available for these configurations. For more information, please contact your AudioCodes sales representative.
- V.150.1 is supported only for the US Department of Defense (DoD).
- *Transcoding Sessions* represents part of the total SBC sessions.
- Conference Participants represents the number of concurrent analog ports in a three-way conference call.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

3.3.4 Mediant 1000B Gateway & E-SBC

This section lists the channel capacity and DSP templates for Mediant 1000B Gateway & E-SBC DSP.

Notes:

- The maximum number of channels on any form of analog, digital, and MPM module assembly is 192. When the device handles both SBC and Gateway call sessions, the maximum number of total sessions is 150. When the device handles SRTP, the maximum capacity is reduced to 120.
- Installation and use of voice coders is subject to obtaining the appropriate license and royalty payments.
- For additional DSP templates, contact your AudioCodes sales representative.

3.3.4.1 Analog (FXS/FXO) Interfaces

The channel capacity per DSP firmware template for analog interfaces is shown in the table below.

Table 3-11: Mediant 1000B Analog Series - Channel Capacity per DSP Firmware Template

	DSP Template	
	0, 1, 2, 4, 5, 6	10, 11, 12, 14, 15, 16
	Number of Channels	
	4	3
Voice Coder		
G.711 A/Mu-law PCM	√	√
G.726 ADPCM	√	√
G.723.1	√	√
G.729 (A / AB)	√	√
G.722	-	√

3.3.4.2 BRI Interfaces

The channel capacity per DSP firmware template for BRI interfaces is shown in the table below.

Table 3-12: Mediant 1000B BRI Series - Channel Capacity per DSP Firmware Template

	DSP Template					
	0, 1, 2, 4, 5, 6			10, 11, 12, 14, 15, 16		
	Number of BRI Spans					
	4	8	20	4	8	20
	Number of Channels					
	8	16	40	6	12	30
Voice Coder						
G.711 A/Mu-law PCM	√			√		
G.726 ADPCM	√			√		
G.723.1	√			√		
G.729 (A / AB)	√			√		
G.722	-			√		

61

3.3.4.3 E1/T1 Interfaces

The channel capacity per DSP firmware template for E1/T1 interfaces is shown in the table below.

Table 3-13: Mediant 1000B E1/T1 Series - Channel Capacity per DSP Firmware Templates

	DSP Template																				
	0 or 10					1 or 11				2 or 12				5 or 15				6 or 16			
	Number of Spans																				
	1	2	4	6	8	1	2	4	6	8	1	2	4	6	8	1	2	4	6	8	1	2	4	6	8
	Number of Channels																				
Default Settings	31	62	120	182	192	31	48	80	128	160	24	36	60	96	120	24	36	60	96	120	31	60	100	160	192
With 128-ms Echo Cancellation	31	60	100	160	192	31	48	80	128	160	24	36	60	96	120	24	36	60	96	120	31	60	100	160	192
With IPM Features	31	60	100	160	192	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	31	60	100	160	192
	Voice Coder																				
G.711 A-Law/M-Law PCM		✓					✓					✓					✓					✓			
G.726 ADPCM		✓					✓					✓					✓					-			
G.723.1		✓					-					-					-					-			
G.729 (A / AB)		✓					✓					✓					✓					✓			
GSM FR		✓					✓					-					-					-			
MS GSM		✓					✓					-					-					-			
iLBC		-					-					-					✓					-			
EVRC		-					-					✓					-					-			
QCELP		-					-					✓					-					-			
MR		-					✓					-					-					-			
M _rR		-					✓					-					-					-			
G.722		-					-					-					-					✓			
Transparent		✓					✓					✓					✓					✓			

> **Note:** "IPM Features" refers to Automatic Gain Control (AGC), Answer Machine Detection (AMD) and Answer Detection (AD).

3.3.4.4 Media Processing Interfaces

The transcoding session capacity according to DSP firmware template (per MPM module) is shown in the table below.

> **Notes:**
> - The device can be housed with up to four MPM modules.
> - The MPM modules can only be housed in slots 1 through 5.

Table 3-14: Transcoding Sessions Capacity per MPM According to DSP Firmware Template for Mediant 1000B

	DSP Template				
	0 or 10	1 or 11	2 or 12	5 or 15	6 or 16
IPM Detectors Automatic Gain Control (AGC), Answer Machine Detection (AMD) and Answer Detection (AD)	Number of Transcoding Sessions per MPM Module				
-	24	16	12	12	20
✓	20	-	-	-	20
	Voice Coder				
G.711 A-law / Mμ-law PCM	✓	✓	✓	✓	✓
G.726 ADPCM	✓	✓	✓	✓	-
G.723.1	✓	-	-	-	-
G.729 (A / AB)	✓	✓	✓	✓	✓
GSM FR	✓	✓	-	-	-
MS GSM	✓	✓	-	-	-
iLBC	-	-	-	✓	-
EVRC	-	-	✓	-	-
QCELP	-	-	✓	-	-
AMR	-	✓	-	-	-
GSM EFR	-	✓	-	-	-
G.722	-	-	-	-	✓
Transparent	✓	✓	✓	✓	✓

3.3.5 MP-1288 Analog Gateway & E-SBC

Session capacity includes Gateway sessions as well as SBC sessions without transcoding capabilities. The maximum capacity of Gateway sessions for MP-1288 Gateway & E-SBC is shown in the table below.

Table 3-15: MP-1288 Gateway - Session Capacity

Coder	Gateway Sessions Capacity	
	Single FXS Blade	Fully Populated (4 x FXS Blades)
Basic: G.711, G.729 (A / AB), G.723.1, G.726 / G.727 ADPCM	72	288
G.722	72	288
AMR-NB	72	288
Opus-NB	60	240

> **Note:**
> - Quality Monitoring and Noise Reduction are not supported.
> - SRTP is supported on all configurations.

3.3.6 Mediant 2600 E-SBC

The maximum number of supported SBC sessions is shown in Section 3.1 on page 49. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below:

Table 3-16: Mediant 2600 E-SBC - Transcoding Capacity per Coder Capability Profile

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Without MPM4	With MPM4
Profile 1	Profile 1	400	600
Profile 2	Profile 1	300	600
Profile 2	Profile 2	250	600
Profile 1	Profile 2 + AMR-NB / G.722	275	600
Profile 2	Profile 2 + AMR-NB / G.722	225	600
Profile 1	Profile 2 + iLBC	175	575
Profile 2	Profile 2 + iLBC	150	500
Profile 1	Profile 2 + AMR-WB (G.722.2)	200	600
Profile 2	Profile 2 + AMR-WB (G.722.2)	175	525
Profile 1	Profile 2 + SILK-NB	200	600
Profile 2	Profile 2 + SILK-NB	175	525
Profile 1	Profile 2 + SILK-WB	100	350
Profile 2	Profile 2 + SILK-WB	100	350
Profile 1	Profile 2 + Opus-NB	125	425
Profile 2	Profile 2 + Opus-NB	125	375
Profile 1	Profile 2 + Opus-WB	100	300
Profile 2	Profile 2 + Opus-WB	75	275

> **Notes:**
> - *Profile 1:* G.711 at 20ms only, with in-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
> - *Profile 2:* G.711, G.726, G.729 (A / AB), G.723.1, T.38 with fax detection, in-band signaling (in voice channel), and Silence Compression.
> - Acoustic Echo Suppressor reduces performance. For more information, contact your AudioCodes sales representative.
> - MPM is the optional, Media Processing Module that provides additional DSPs, allowing greater capacity.

3.3.7 Mediant 4000 SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 49. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

Table 3-17: Mediant 4000 SBC - Transcoding Capacity per Coder Capability Profile

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Without MPM8	With MPM8
Profile 1	Profile 1	800	2,400
Profile 2	Profile 1	600	1,850
Profile 2	Profile 2	500	1,550
Profile 1	Profile 2 + AMR-NB / G.722	550	1,650
Profile 2	Profile 2 + AMR-NB / G.722	450	1,350
Profile 1	Profile 2 + iLBC	350	1,150
Profile 2	Profile 2 + iLBC	300	1,000
Profile 1	Profile 2 + AMR-WB (G.722.2)	400	1,200
Profile 2	Profile 2 + AMR-WB (G.722.2)	350	1,050
Profile 1	Profile 2 + SILK-NB	400	1,200
Profile 2	Profile 2 + SILK-NB	350	1,050
Profile 1	Profile 2 + SILK-WB	200	700
Profile 2	Profile 2 + SILK-WB	200	700
Profile 1	Profile 2 + Opus-NB	250	850
Profile 2	Profile 2 + Opus-NB	250	750
Profile 1	Profile 2 + Opus-WB	200	600
Profile 2	Profile 2 + Opus-WB	150	550

Notes:
- *Profile 1*: G.711 at 20ms only, with in-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
- *Profile 2*: G.711, G.726, G.729 (A / AB), G.723.1, T.38 with fax detection, in-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance. For more information, contact your AudioCodes sales representative.
- MPM is the optional, Media Processing Module that provides additional DSPs, allowing greater capacity.

3.3.7.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

Table 3-18: Mediant 4000 SBC - Forwarding Capacity per Feature

Feature	Max. Sessions
Fax Detection	5,000
AD/AMD/Beep Detection	5,000
CP Detection	5,000
Jitter Buffer	5,000

Notes:
- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - Timeout for fax detection is 10 seconds (default)
  - Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

3.3.8 Mediant 4000B SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 49. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

Table 3-19: Mediant 4000B SBC - Transcoding Capacity per Coder Capability Profile

Session Coders		Max. Sessions				
From Coder Profile	To Coder Profile	Without MPM	1 x MPM8B	1 x MPM12B	2 x MPM12B	3 x MPM12B
Profile 1	Profile 1	800	2,400	3,250	5,000	5,000
Profile 2	Profile 1	600	1,850	2,450	4,350	5,000
Profile 2	Profile 2	500	1,550	2,100	3,650	5,000
Profile 1	Profile 2 + AMR-NB / G.722	550	1,650	2,200	3,850	5,000
Profile 2	Profile 2 + AMR-NB / G.722	450	1,350	1,800	3,150	4,550
Profile 1	Profile 2 + iLBC	400	1,200	1,600	2,850	4,050
Profile 2	Profile 2 + iLBC	350	1,050	1,400	2,500	3,600
Profile 1	Profile 2 + AMR-WB (G.722.2)	400	1,200	1,600	2,850	4,050
Profile 2	Profile 2 + AMR-WB (G.722.2)	350	1,050	1,400	2,500	3,600
Profile 1	Profile 2 + SILK-NB	400	1,200	1,600	2,850	4,050
Profile 2	Profile 2 + SILK-NB	350	1,050	1,400	2,500	3,600
Profile 1	Profile 2 + SILK-WB	200	700	950	1,650	2,400
Profile 2	Profile 2 + SILK-WB	200	700	950	1,650	2,400
Profile 1	Profile 2 + Opus-NB	250	850	1,150	2,000	2,850
Profile 2	Profile 2 + Opus-NB	250	750	1,050	1,800	2,600

Session Coders		Max. Sessions				
From Coder Profile	To Coder Profile	Without MPM	1 x MPM8B	1 x MPM12B	2 x MPM12B	3 x MPM12B
Profile 1	Profile 2 + Opus-WB	200	600	850	1,500	2,150
Profile 2	Profile 2 + Opus-WB	150	550	750	1,300	1,900

Notes:
- *Profile 1*: G.711 at 20ms only, with In-band signaling (in voice channel), DTMF transcoding (RFC 2833 to in-band signaling), and Silence Suppression (no fax detection or T.38 support).
- *Profile 2*: G.711, G.726, G.729 (A / AB), G.723.1, AMR-NB, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance by about 30%. For more information, contact your AudioCodes sales representative.
- MPM8 is the optional, Media Processing Module that provides additional DSPs, allowing greater capacity.

3.3.8.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

Table 3-20: Mediant 4000B SBC - Forwarding Capacity per Feature

Feature	Max. Sessions
Fax Detection	5,000
AD/AMD/Beep Detection	5,000
CP Detection	5,000
Jitter Buffer	5,000

Notes:
- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - Timeout for fax detection is 10 seconds (default)
  - Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

3.3.9 Mediant 9000 SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 49. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

Table 3-21: Mediant 9000 SBC - Transcoding Capacity per Coder Capability Profile

Session Coders		Max. Sessions			
From Coder Profile	To Coder Profile	Without Hyper-Threading		With Hyper-Threading	
		Basic	Extended	Basic	Extended
Profile 1	Profile 1	3,025	2,525	6,575	3,875
Profile 2	Profile 1	1,500	1,325	2,125	1,700
Profile 2	Profile 2	1,000	900	1,275	1,100
Profile 1	Profile 2 + AMR-NB / G.722	1,500	1,300	2,075	1,625
Profile 2	Profile 2 + AMR-NB / G.722	1,000	900	1,225	1,050
Profile 1	Profile 2 + AMR-WB (G.722.2)	500	475	600	575
Profile 2	Profile 2 + AMR-WB	425	400	500	475
Profile 1	Profile 2 + SILK-NB	1,300	1,175	1,700	1,450
Profile 2	Profile 2 + SILK-NB	900	825	1,100	975
Profile 1	Profile 2 + SILK-WB	775	750	1,000	950
Profile 2	Profile 2 + SILK-WB	625	600	750	725
Profile 1	Profile 2 + Opus-NB	825	750	1,050	900
Profile 2	Profile 2 + Opus-NB	650	600	775	700
Profile 1	Profile 2 + Opus-WB	625	575	800	700
Profile 2	Profile 2 + Opus-WB	525	475	625	575

Notes:
- *Profile 1*: G.711 at 20ms only, without T.38 support.
- *Profile 2*: G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection.
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

G3

3.3.9.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

Table 3-22: Mediant 9000 SBC - Forwarding Capacity per Feature

Feature	Max. Sessions	
	Without Hyper-Threading	With Hyper-Threading
Fax Detection	24,000	40,000
AD/AMD/Beep Detection	24,000	39,000
CP Detection	24,000	44,000
Jitter Buffer	2,225	5,000

Notes:
- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - √ Timeout for fax detection is 10 seconds (default)
  - √ Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

3.3.10 Mediant 9000 Rev. B / 9080 SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 49. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

Table 3-23: Mediant 9000 Rev. B / 9080 - Transcoding Capacity per Coder Capability Profile

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	9,600	6,625
Profile 2	Profile 1	4,400	3,625
Profile 2	Profile 2	2,875	2,500
Profile 1	Profile 2 + AMR-NB / G.722	2,925	2,600
Profile 2	Profile 2 + AMR-NB / G.722	2,150	1,950
Profile 1	Profile 2 + AMR-WB (G.722.2)	950	925
Profile 2	Profile 2 + AMR-WB	850	825
Profile 1	Profile 2 + SILK-NB	2,750	2,500
Profile 2	Profile 2 + SILK-NB	2,050	1,900
Profile 1	Profile 2 + SILK-WB	1,575	1,475
Profile 2	Profile 2 + SILK-WB	1,300	1,250
Profile 1	Profile 2 + Opus-NB	1,700	1,450
Profile 2	Profile 2 + Opus-NB	1,375	1,200
Profile 1	Profile 2 + Opus-WB	1,375	1,200
Profile 2	Profile 2 + Opus-WB	1,175	1,025

Notes:
- *Profile 1*: G.711 at 20ms only, without T.38 support.
- *Profile 2*: G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

3.3.10.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

Table 3-24: Mediant 9000 Rev. B / 9080 SBC - Forwarding Capacity per Feature

Feature	Max. Sessions
Fax Detection	45,000
AD, AMD, and Beep Detection	45,000
CP Detection	45,000
Jitter Buffer	6,000

Notes:
- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - √ Timeout for fax detection is 10 seconds (default)
  - √ Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

3.3.11 Mediant 9000 / 9000 Rev. B / 9080 SBC with Media Transcoders

Mediant 9000, Mediant 9000 Rev. B, or Mediant 9080 SBC with Media Transcoders allows increasing the number of transcoding sessions by using Media Transcoders. The maximum number of transcoding sessions depends on the following:

- Number of Media Transcoders in the media transcoding cluster.
- Cluster operation mode (Best-Effort or Full-HA mode).
- Maximum transcoding sessions. Each transcoding session is weighted as two RTP-RTP sessions without transcoding. Therefore, the number of sessions without transcoding plus the doubled number of sessions with transcoding must be less than the maximum RTP-RTP value specified in the table. As a result, if all sessions are with transcoding, the maximum number of sessions is half the maximum RTP-RTP sessions without transcoding as specified in Table 3-1.

The following table lists maximum transcoding sessions capacity of a single Media Transcoder.

Table 3-25: Single Media Transcoder (MT) - Transcoding Capacity per Profile

Session Coders		Max. Sessions		
From Coder Profile	To Coder Profile	1 x MPM12B	2 x MPM12B	3 x MPM12B
Profile 1	Profile 1	2,875	5,000	5,000
Profile 2	Profile 1	2,300	4,025	5,000
Profile 2	Profile 2	1,800	3,175	4,550
Profile 1	Profile 2 + AMR-NB / G.722	2,000	3,525	5,000

Session Coders		Max. Sessions		
From Coder Profile	To Coder Profile	1 x MPM12B	2 x MPM12B	3 x MPM12B
Profile 2	Profile 2 + AMR-NB / G.722	1,625	2,850	4,075
Profile 1	Profile 2 + AMR-WB (G.722.2)	1,425	2,500	3,600
Profile 2	Profile 2 + AMR-WB (G.722.2)	1,225	2,175	3,100
Profile 1	Profile 2 + SILK-NB	1,425	2,500	3,600
Profile 2	Profile 2 + SILK-NB	1,225	2,175	3,100
Profile 1	Profile 2 + SILK-WB	850	1,500	2,150
Profile 2	Profile 2 + SILK-WB	850	1,500	2,150
Profile 1	Profile 2 + Opus-NB	1,050	1,825	2,625
Profile 2	Profile 2 + Opus-NB	950	1,675	2,400
Profile 1	Profile 2 + Opus-WB	750	1,325	1,900
Profile 2	Profile 2 + Opus-WB	650	1,175	1,675

Notes:
- *Profile 1*: G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2*: G.711, G.726, G.729 (A / AB), G.723.1, AMR-NB, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance by about 30%. For more information, contact your AudioCodes sales representative.
- MPM12B is a Media Processing Module in the Media Transcoder that provides additional DSPs, allowing higher capacity.
- For best cluster efficiency, all Media Transcoders in the Cluster should populate the same number of MPM12Bs.
- The SBC employs load balancing of transcoding sessions among all Media Transcoders in the Cluster. Each Media Transcoder can handle up to 200 calls (transcoded sessions) per second (CPS).

64

3.3.12 Mediant 9030 SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 49. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

Table 3-26: Mediant 9030 SBC - Transcoding Capacity per Coder Capability Profile

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	4,025	2,775
Profile 2	Profile 1	1,825	1,525
Profile 2	Profile 2	1,200	1,050
Profile 1	Profile 2 + AMR-NB / G.722	1,200	1,075
Profile 2	Profile 2 + AMR-NB / G.722	875	825
Profile 1	Profile 2 + AMR-WB (G.722.2)	400	375
Profile 2	Profile 2 + AMR-WB	350	350
Profile 1	Profile 2 + SILK-NB	1,150	1,050
Profile 2	Profile 2 + SILK-NB	850	775
Profile 1	Profile 2 + SILK-WB	650	625
Profile 2	Profile 2 + SILK-WB	525	525
Profile 1	Profile 2 + Opus-NB	700	600
Profile 2	Profile 2 + Opus-NB	575	500
Profile 1	Profile 2 + Opus-WB	575	500
Profile 2	Profile 2 + Opus-WB	475	425

Notes:
- *Profile 1*: G.711 at 20ms only, without T.38 support.
- *Profile 2*: G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

3.3.12.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

Table 3-27: Mediant 9030 SBC - Forwarding Capacity per Feature

Feature	Max. Sessions
Fax Detection	23,000
AD/AMD/Beep Detection	23,000
CP Detection	23,000
Jitter Buffer	3,000

Notes:
- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - Timeout for fax detection is 10 seconds (default)
  - Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

3.3.13 Mediant Cloud Edition (CE) SBC

The Media Components (MC) in the media cluster of the Mediant CE must all be of the same instance type: either forwarding-only, or forwarding and transcoding. A maximum of 21 MCs can be used.

3.3.13.1 Mediant CE SBC for AWS EC2

3.3.13.1.1 Forwarding Sessions

The number of concurrent forwarding sessions per MC is shown in the following table.

Table 3-28: Forwarding Capacity per MC Instance Type

MC Instance Type	Max. Forwarding Sessions
m5.large	6,000
c5.4xlarge	4,000

Note: Forwarding performance was tested in AWS Ireland Region.

3.3.13.1.2 Transcoding Sessions

For transcoding capabilities, the Media Component (MC) must be of the AWS instance type c5.4xlarge. The number of supported transcoding sessions per MC is shown in the following table.

Table 3-29: Transcoding Capacity per c5.4xlarge MC

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	4,000	2,825
Profile 2	Profile 1	2,375	1,900
Profile 2	Profile 2	1,625	1,425
Profile 1	Profile 2 + AMR-NB / G.722	1,500	1,300
Profile 2	Profile 2 + AMR-NB / G.722	1,150	1,050
Profile 1	Profile 2 + AMR-WB (G.722.2)	475	475
Profile 2	Profile 2 + AMR-WB	425	425
Profile 1	Profile 2 + SILK-NB	1,400	1,250
Profile 2	Profile 2 + SILK-NB	1,100	1,025
Profile 1	Profile 2 + SILK-WB	775	750
Profile 2	Profile 2 + SILK-WB	675	675
Profile 1	Profile 2 + Opus-NB	850	725
Profile 2	Profile 2 + Opus-NB	725	650

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 2 + Opus-WB	700	600
Profile 2	Profile 2 + Opus-WB	625	550

Notes:
- *Profile 1*: G.711 at 20ms only, without T.38 support.
- *Profile 2*: G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

3.3.13.2 Mediant CE SBC for Azure

3.3.13.2.1 Forwarding Sessions

The number of concurrent forwarding sessions per Media Component (MC) is shown in the following table.

Table 3-30: Session Capacity per MC

MC VM Size	Max. Forwarding-Only Sessions	Max. Forwarding & Transcoding Sessions
DS2_v2	1,200	900
DS3_v2	1,700	1,100
DS4_v2	1,800	1,600

3.3.13.2.2 Transcoding Sessions

For transcoding capabilities, the Media Component (MC) must be of the Azure DS2_v2 / DS3_v2 / DS4_v2 virtual machine size. The number of supported transcoding sessions per MC is shown in the following table.

Table 3-31: Transcoding Capacity per MC

Session Coders		DS2_v2		DS3_v2		DS4_v2	
From Coder Profile	To Coder Profile	Basic	Extended	Basic	Extended	Basic	Extended
Profile 1	Profile 1	175	175	575	575	1,175	1,175
Profile 2	Profile 1	100	100	325	300	675	600
Profile 2	Profile 2	75	50	225	200	450	400
Profile 1	Profile 2 + AMR-NB / G.722	100	100	325	300	675	600
Profile 2	Profile 2 + AMR-NB / G.722	75	50	225	200	450	400
Profile 1	Profile 2 + AMR-WB (G.722.2)	25	25	100	100	225	200
Profile 2	Profile 2 + AMR-WB	25	25	75	75	175	175
Profile 1	Profile 2 + SILK-NB	100	75	300	250	600	525
Profile 2	Profile 2 + SILK-NB	50	50	200	175	400	375
Profile 1	Profile 2 + SILK-WB	50	50	175	150	350	325
Profile 2	Profile 2 + SILK-WB	25	25	125	125	275	275
Profile 1	Profile 2 + Opus-NB	50	50	175	175	375	350
Profile 2	Profile 2 + Opus-NB	25	25	125	125	275	275
Profile 1	Profile 2 + Opus-WB	25	25	125	125	275	250
Profile 2	Profile 2 + Opus-WB	25	25	100	100	225	225

3.3.13.3 Mediant CE SBC for VMware

The following tables list maximum transcoding capacity for Mediant CE SBC running on VMware hypervisor with Hyper-Threading.

Each vCPU refers to a single thread of a physical core. For example, a 4-vCPU virtual machine is allocated by only two physical cores.

Note:
- The profiles below require the following minimum requirements:
  - √ Intel Xeon Scalable Processors or later. The capacity listed in the following table refers to 3.3 GHz all-core Turbo speed. When using different all-core Turbo speed, capacity is increased or decreased accordingly.
  - √ Hyper-Threading is enabled on host.
  - √ VMware ESXi 6.7 or later.
  - √ CPUOverrideHT ini file parameter is configured to 1.
- CPU Affinity is recommended. For more information, refer to the *Installation Manual*.
- For Server Failure redundancy, the maximum media sessions on each server must not exceed 4,000 media sessions.

3.3.13.3.1 Forwarding Sessions

The number of concurrent forwarding sessions per Media Component (MC) is shown in the following table.

Table 3-32: Forwarding Capacity per MC Instance Type

MC Instance Type	Max. Sessions
2 vCPUs, 8GB	4,000 (Forwarding Only)
8 vCPUs, 8GB	4,000 (Forwarding and Transcoding)

3.3.13.3.2 Transcoding Sessions

For transcoding capabilities, the Media Component (MC) must be a virtual machine of 8 vCPUs and 8 GB. The number of supported transcoding sessions per MC is shown in the following table.

Note: For transcoding capabilities, the 'Media Component Profile' parameter on all Media Components must be configured to **Transcoding Enabled** (MCProfile = 1).

Table 3-33: Mediant CE SBC on VMware with Hyper-Threading - Transcoding Capacity

Session Coders		Max. Sessions 8 vCPU 8-GB RAM	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	1,800	1,175
Profile 1	Profile 2	975	775
Profile 2	Profile 2	675	575
Profile 1	Profile 2 + SILK-NB	575	525
Profile 2	Profile 2 + SILK-NB	450	425
Profile 1	Profile 2 + AMR-WB	200	175
Profile 2	Profile 2 + AMR-WB	175	175
Profile 1	Profile 2 + G.722 / AMR-NB	600	525
Profile 2	Profile 2 + G.722 / AMR-NB	475	425
Profile 1	Profile 2 + SILK-WB	325	300
Profile 2	Profile 2 + SILK-WB	275	275
Profile 1	Profile 2 + Opus-NB	350	300
Profile 2	Profile 2 + Opus-NB	300	275
Profile 1	Profile 2 + Opus-WB	300	250
Profile 2	Profile 2 + Opus-WB	250	225

3.3.14 Mediant Virtual Edition (VE) SBC

The maximum number of supported SBC sessions is listed in Section 3.1 on page 49. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required (DSP Performance Profile), the number of sessions that can use DSP capabilities is reduced, as shown in the tables in this section.

3.3.14.1 Mediant VE SBC for Hypervisors with Hyper-Threading

The following tables list maximum transcoding capacity for Mediant VE SBC running on the following hypervisors with Hyper-Threading: VMware, KVM/OpenStack, and Hyper-V.

Each vCPU refers to a Hyper-Threaded core (logical). For example, a 4-vCPU virtual machine allocates only 2 physical cores.

Note:
- The transcoding profiles below require the following minimum requirements:
  - √ Intel Xeon Scalable Processors or later. The capacity listed in the table below refer to 3.3 GHz all-core Turbo speed. When using different all-core Turbo speed, the capacity is increased or decreased accordingly.
  - √ Hyper-Threading enabled on host.
  - √ VMware Hypervisor:
    - o VMware ESXi 6.7 or later.
    - o CPUOverrideHT ini file parameter is configured to 1.
  - √ KVM Hypervisor/OpenStack: Host-Passthrough mode must be used. For more information, refer to the *Installation Manual*.
- CPU Affinity is recommended. For more information, refer to the *Installation Manual*.
- For transcoding capabilities, the 'SBC Performance Profile' (SBCPerformanceProfile) parameter must be configured to Optimized for Transcoding (2).

Table 3-34: Mediant VE SBC on Hypervisors with Hyper-Threading - Transcoding Capacity

Session Coders		Max. Sessions							
		2 vCPU 8-GB RAM		4 vCPU 8-GB RAM (VMware Only)		8 vCPU 16-GB RAM		16 vCPU 16-GB RAM (Not Hyper-V)	
From Coder Profile	To Coder Profile	Basic	Extended	Basic	Extended	Basic	Extended	Basic	Extended
Profile 1	Profile 1	300	200	800	600	1200	825	2,400	2,400
Profile 1	Profile 2	150	125	500	400	675	550	2,075	1,650
Profile 2	Profile 2	100	100	350	300	475	400	1,425	1,250
Profile 1	Profile 2 + SILK-NB	100	75	300	275	400	350	1,225	1,100
Profile 2	Profile 2 + SILK-NB	75	75	225	225	325	300	975	900
Profile 1	Profile 2 + AMR-WB	25	25	100	100	125	125	425	400
Profile 2	Profile 2 + AMR-WB	25	25	75	75	125	125	375	375

Session Coders		Max. Sessions							
		2 vCPU 8-GB RAM		4 vCPU 8-GB RAM (VMware Only)		8 vCPU 16-GB RAM		16 vCPU 16-GB RAM (Not Hyper-V)	
From Coder Profile	To Coder Profile	Basic	Extended	Basic	Extended	Basic	Extended	Basic	Extended
Profile 1	Profile 2 + G.722 / AMR-NB	100	75	325	275	425	375	1,300	1,150
Profile 2	Profile 2 + G.722 / AMR-NB	75	75	250	225	325	300	1,000	925
Profile 1	Profile 2 + SILK-WB	50	50	175	150	225	200	700	650
Profile 2	Profile 2 + SILK-WB	50	50	150	150	200	200	600	600
Profile 1	Profile 2 + Opus-NB	50	50	175	150	250	200	750	650
Profile 2	Profile 2 + Opus-NB	50	25	150	125	200	175	650	575
Profile 1	Profile 2 + Opus-WB	50	25	150	125	200	175	625	525
Profile 2	Profile 2 + Opus-WB	25	25	125	100	175	150	550	475

3.3.14.2 Mediant VE SBC for Amazon AWS EC2

The following tables list maximum channel capacity for Mediant VE SBC on the Amazon EC2 platform.

Table 3-35: Mediant VE SBC on c5.2xlarge - Transcoding Capacity

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	1950	1275
Profile 2	Profile 1	1050	850
Profile 2	Profile 2	725	625
Profile 1	Profile 2 + AMR-NB / G.722	675	575
Profile 2	Profile 2 + AMR-NB / G.722	500	475
Profile 1	Profile 2 + AMR-WB	200	200
Profile 2	Profile 2 + AMR-WB	175	175
Profile 1	Profile 2 + SILK-NB	625	550
Profile 2	Profile 2 + SILK-NB	500	450
Profile 1	Profile 2 + SILK-WB	350	325
Profile 2	Profile 2 + SILK-WB	300	300
Profile 1	Profile 2 + Opus-NB	375	325

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 2	Profile 2 + Opus-NB	325	300
Profile 1	Profile 2 + Opus-WB	300	275
Profile 2	Profile 2 + Opus-WB	275	250

Table 3-36: Mediant VE SBC on c5.9xlarge - Transcoding Capacity

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	7,000	6,800
Profile 2	Profile 1	5,725	4,575
Profile 2	Profile 2	3,925	3,450
Profile 1	Profile 2 + AMR-NB / G.722	3,600	3,125
Profile 2	Profile 2 + AMR-NB / G.722	2,775	2,550
Profile 1	Profile 2 + AMR-WB	1,175	1,150
Profile 2	Profile 2 + AMR-WB	1,050	1,000
Profile 1	Profile 2 + SILK-NB	3,400	3,025
Profile 2	Profile 2 + SILK-NB	2,675	2,475
Profile 1	Profile 2 + SILK-WB	1,900	1,800
Profile 2	Profile 2 + SILK-WB	1,650	1,625
Profile 1	Profile 2 + Opus-NB	2,075	1,775
Profile 2	Profile 2 + Opus-NB	1,775	1,600
Profile 1	Profile 2 + Opus-WB	1,725	1,450
Profile 2	Profile 2 + Opus-WB	1,500	1,325

Notes:
- *Profile 1*: G.711 at 20ms only, without T.38 support.
- *Profile 2*: G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

3.3.14.2.1.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

Table 3-37: Mediant VE SBC on Amazon EC2 - Forwarding Capacity per Feature

Feature	Max. Sessions	
	c5.2xlarge	c5.9xlarge
Fax Detection	5,500	7,000
AD/AMD/Beep Detection	5,500	7,000
CP Detection	5,500	7,000
Jitter Buffer	1,800	7,000

Notes:
- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - Timeout for fax detection is 10 seconds (default)
  - Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

3.3.14.3 Mediant VE SBC for Azure

The following tables list maximum channel capacity for Mediant VE SBC on the Azure platform.

Table 3-38: Mediant VE SBC on DS1_v2, DS2_v2, DS3_ v2 & DS4_v2 - Transcoding Capacity

Session Coders		Max. Sessions					
		DS1_v2 and DS2_v2		DS3_v2		DS4_v2	
From Coder Profile	To Coder Profile	Basic	Extended	Basic	Extended	Basic	Extended
Profile 1	Profile 1	200	200	625	600	1,025	1,025
Profile 2	Profile 1	100	100	350	325	600	525
Profile 2	Profile 2	75	50	225	200	400	350
Profile 1	Profile 2 + AMR-NB / G.722	100	100	350	300	600	525
Profile 2	Profile 2 + AMR-NB / G.722	75	50	225	200	400	350
Profile 1	Profile 2 + AMR-WB (G.722.2)	25	25	100	100	200	175
Profile 2	Profile 2 + AMR-WB	25	25	100	75	175	150
Profile 1	Profile 2 + SILK-NB	100	75	300	275	525	475
Profile 2	Profile 2 + SILK-NB	50	50	200	200	350	325
Profile 1	Profile 2 + SILK-WB	50	50	175	175	300	300
Profile 2	Profile 2 + SILK-WB	50	25	150	125	250	225
Profile 1	Profile 2 + Opus-NB	50	50	200	175	325	300
Profile 2	Profile 2 + Opus-NB	50	50	150	150	250	250
Profile 1	Profile 2 + Opus-WB	50	25	150	125	250	225
Profile 2	Profile 2 + Opus-WB	25	25	125	100	200	200

67

3.3.15 Mediant Server Edition (SE) SBC

> **Note:** Digital signal processing (DSP) is supported only on Mediant SE SBC based on DL360 G10.

The maximum number of supported SBC sessions is listed in Section 3.1 on page 49. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below.

Table 3-39: Mediant SE SBC (DL360 G10) - Transcoding Capacity per Coder Capability Profile

Session Coders		Max. Sessions	
From Coder Profile	To Coder Profile	Basic	Extended
Profile 1	Profile 1	9,600	6,625
Profile 2	Profile 1	4,400	3,625
Profile 2	Profile 2	2,875	2,500
Profile 1	Profile 2 + AMR-NB / G.722	2,925	2,600
Profile 2	Profile 2 + AMR-NB / G.722	2,150	1,950
Profile 1	Profile 2 + AMR-WB (G.722.2)	950	925
Profile 2	Profile 2 + AMR-WB	850	825
Profile 1	Profile 2 + SILK-NB	2,750	2,500
Profile 2	Profile 2 + SILK-NB	2,050	1,900
Profile 1	Profile 2 + SILK-WB	1,575	1,475
Profile 2	Profile 2 + SILK-WB	1,300	1,250
Profile 1	Profile 2 + Opus-NB	1,700	1,450
Profile 2	Profile 2 + Opus-NB	1,375	1,200
Profile 1	Profile 2 + Opus-WB	1,375	1,200
Profile 2	Profile 2 + Opus-WB	1,175	1,025

Notes:
- *Profile 1*: G.711 at 20ms only, without T.38 support.
- *Profile 2*: G.711, G.726, G.729 (A / AB), G.723.1, T.38.
- *Basic*: Excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: Includes DTMF transcoding (RFC 2833 to in-band signaling), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

3.3.15.1 Forwarding Session Capacity per Feature without Transcoding

The table below lists the maximum number of concurrent forwarding sessions per feature without using transcoding.

Table 3-40: Mediant SE SBC (DL360 G10) - Forwarding Capacity per Feature

Feature	Max. Sessions
Fax Detection	45,000
AD/AMD/Beep Detection	45,000
CP Detection	45,000
Jitter Buffer	6,000

Notes:
- All figures were calculated for call duration of 100 seconds.
- For fax detection, figures are based on the following assumptions:
  - Timeout for fax detection is 10 seconds (default)
  - Fax detection is required on both legs of the call
- Figures for Call Progress (CP), AD, AMD, and Beep detection assume that detection is only on one leg of the call (if not, figures will be reduced).

3.4 Configuration Table Capacity

The maximum rows (indices) that can be configured per configuration table is listed in the table below.

Table 3-41: Capacity per Configuration Table

Configuration Table	MP-1288 / Mediant 500/500L/800/1000B	Mediant 2600/4000B	Mediant 90xx/SE	Mediant VE/CE
Access List	10	10	10	10
ounts	102	625	1,500	1,500
tional Management ...erfaces	16	64	64	64
Allowed Audio Coders Groups	10	20	20	20
Allowed Video Coders Groups	5	5	5	5
Alternative Routing Reasons	20	20	20	20
Bandwidth Profile	486	1,009	1,884	1,884
Call Admission Control Profile	102	1,500	1,500	1,500
Call Admission Control Rule (per Profile)	8	8	8	8
Call Setup Rules	64 (MP-1288; Mediant 1000) 100 (Mediant 500/500L/800)	400	1,000	• 2-8 GB: 500 • 16-64 GB: 1,000
Calling Name Manipulation for IP-to-Tel Calls	120	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Calling Name Manipulation for Tel-to-IP Calls	120	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Char Conversion	40	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Charge Codes	25	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Classification	102	625	1,500	• 2 GB: 750 • 3.5-64 GB: 1,500
Coder Groups	11	21	21	21
Cost Groups	10	10	10	10
Destination Phone Number Manipulation for IP-to-Tel Calls	120	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Destination Phone Number Manipulation for Tel-to-IP Calls	120	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
DHCP Servers	1	1	1	1
Dial Plan	10	25	50	50
Dial Plan Rule	2,000	10,000	100,000	• < 16 GB: 2,000 • > 16 GB: 100,000
Ethernet Devices	16	1,024	1,024	1,024

Configuration Table	MP-1288 / Mediant 500/500L/800/1000B	Mediant 2600/4000B	Mediant 90xx/SE	Mediant VE/CE
External Media Source	1	1	1	1
Firewall	50	500	500	500
Forward On Busy Trunk Destination		n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Gateway CDR Format	128 (Syslog); 40 (RADIUS); 64 (Locally Stored & JSON)	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
HA Network Monitor	10	10	10	10
HTTP Directive Sets	30	30	30	30
HTTP Directives	500	500	500	500
HTTP Locations	40	40	40	40
HTTP Proxy Servers	10	10	10	10
HTTP Remote Hosts	10 (per Remote Web Service)	10 (per Remote Web Service)	10 (per Remote Web Service)	10 (per Remote Web Service)
IDS Matches	20	20	20	20
IDS Policies	20	20	20	20
IDS Rule	100 (20 per Policy)	100 (20 per Policy)	100 (20 per Policy)	100 (20 per Policy)
Inbound Manipulations	205	3,000	3,000	3,000
Internal DNS	20	20	20	20
Internal SRV	10	10	10	10
IP Group Set	51	350	2,500	• 2 GB: 40 • 3.5 GB: 500 • 4-16 GB: 750 • 32-64 GB: 2,500
IP Groups	80	700	5,000	• 2 GB: 80 • 3.5 GB: 1,000 • 4-16 GB: 1,500 • 32-64 GB: 5,000
IP Interfaces	12	1,024	1,024	1,024
IP Profiles	20 (MP-1288 / Mediant 500/L / Mediant 800); 40 (Mediant 1000)	125	300 (Mediant 9030); 1,500 (Mediant 9000/9080/SE)	• 2 GB: 150 • 5-32 GB: 300 • 64 GB: 1,500
IP-to-IP Routing	615	9,000	9,000	• 2 GB: 4500 • 3.5-64 GB: 9,000
IP-to-Tel Routing	120	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
LDAP Server Groups	41	600	600	600
LDAP Servers	82	1,200	1,200	1,200

Configuration Table	MP-1288 / Mediant 500/500L/800/1000B	Mediant 2600/4000B	Mediant 90xx/SE	Mediant VE/CE
Local Users	20	20	20	20
Logging Filters	60	60	60	60
Malicious Signature	20	20	20	20
Media Realm Extension	2 x Max. Media Realms (MP-1288, Mediant 500, Mediant 500L, Mediant 800 Only)	2 x Max. Media Realms (Mediant 2600) 5 x Max. Media Realms (Mediant 4000B)	5 x Max. Media Realms	5 x Max. Media Realms
Media Realms	12	1,024	1,024	1,024
Message Conditions	82	1,200	1,200	1,200
Message Manipulations	100 (MP-1288 / Mediant 500/L / Mediant 800); 200 (Mediant 1000)	500	500	500
Message Policies	20	20	20	20
NAT Translation	32	32	32	32
Outbound Manipulations	205	3,000	3,000	3,000
OVOC Services	1	1	1	1
Phone Contexts	20	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Pre-Parsing Manipulation Rules	30	30	30	30
Pre-Parsing Manipulation Sets	10	10	10	10
Proxy Address (and DNS-resolved IP addresses) per Proxy Set	10 (15 DNS-resolved IP addresses)	10 (15 DNS-resolved IP addresses)	50 (50 DNS-resolved IP addresses)	• 2 GB: 10 (15 DNS-resolved IP addresses) • 3.5 GB: 1,000 • 8-16 GB: 10 (50 DNS-resolved IP addresses) • 32-64 GB: 50 (50 DNS-resolved IP addresses)
ly Sets	80	700	5,000	• 2 GB: 80 • 3.5 GB: 10 • 4-16 GB: 1,500 • 32-64 GB: 5,000
QoS Mapping	64	64	64	64
Quality of Experience Color Rules	256	256	256	256
Quality of Experience Profile	256	256	256	256
Quality Of Service Rules	510	3,500	7,500	7,500
RADIUS Servers	3	3	3	3

Configuration Table	MP-1288 / Mediant 500/500L/800/1000B	Mediant 2600/4000B	Mediant 90xx/SE	Mediant VE/CE
Reasons for IP-to-Tel Alternative Routing	10	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Reasons for Tel-to-IP Alternative Routing	10	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Redirect Number IP-to-Tel	20	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Redirect Number Tel-to-IP	20	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Release Cause ISDN->ISDN	10	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Release Cause Mapping from ISDN to SIP	12	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Release Cause Mapping from SIP to ISDN	12	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Remote Media Subnet	5	5	5	5
Remote Web Services	7	7	7	7
Routing Policies	20 (SBC)	600	600	• 2 GB: 20 • 3.5 GB: 70 • 4 GB: 100 • 8 GB: 200 • 16 GB: 400 • 32-64 GB: 600
Routing Policies	1 (Gateway)	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
SBC CDR Format	128 (Syslog); 40 (RADIUS); 64 (Locally Stored & JSON)	128 (Syslog); 128 (RADIUS); 64 (Locally Stored & JSON)	128 (Syslog); 128 (RADIUS); 64 (Locally Stored & JSON)	128 (Syslog); 128 (RADIUS); 64 (Locally Stored & JSON)
SIP Interfaces	80	700	1,200	• 2 GB: 40 • 3 GB: 200 • 4 GB: 400 • 8 GB: 800 • 16 GB: 1,200 • 32-64 GB: 1,200
SIP Recording Rules	30	30	30	30
SNMP Trap Destinations	5	5	5	5
SNMP Trusted Managers	5	5	5	5
SNMPv3 Users	10	10	10	10
Source Phone Number Manipulation for IP-to-Tel Calls	120	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)

Configuration Table	MP-1288 / Mediant 500/500L/800/1000B	Mediant 2600/4000B	Mediant 90xx/SE	Mediant VE/CE
Source Phone Number Manipulation for Tel-to-IP Calls	120	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
SRDs	20	600	600	• 2 GB: 20 • 3.5 GB: 70 • 4 GB: 100 • 8 GB: 200 • 16 GB: 400 • 32-64 GB: 600
atic Routes	30	30	30	30
Supplementary Services	100	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
TCP/UDP Proxy Servers	10	10	10	10
Tel Profiles	9	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Tel-to-IP Routing	180	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Test Call Rules	5 (default)	5 (default)	5 (default)	5 (default)
Time Band	70 (21 per Cost Group)	70 (21 per Cost Group)	70 (21 per Cost Group)	70 (21 per Cost Group)
TLS Contexts	12 (15 for Mediant 1000)	100	100	100
Tone Index	50	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Trunk Group	288 (MP-1288); 24 (Mediant 500/L; Mediant 800); 240 (Mediant 1000)	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Trunk Group Settings	289 (MP-1288); 101 (Mediant 500/L; Mediant 800); 241 (Mediant 1000)	n/a (Gateway only)	n/a (Gateway only)	n/a (Gateway only)
Upstream Groups	10	10	10	10
Upstream Hosts	50 (5 per Upstream Group)	50 (5 per Upstream Group)	50 (5 per Upstream Group)	50 (5 per Upstream Group)

4 Supported SIP Standards

This section lists SIP RFCs and standards supported by the device.

4.1 Supported SIP RFCs

The table below lists the supported RFCs.

Table 4-1: Supported RFCs

RFC	Description	Gateway	SBC
draft-choudhuri-sip-info-digit-00	SIP INFO method for DTMF digit transport and collection	√	√
draft-ietf-bfcpbis-rfc4583bis-12	Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams	×	√ (forwarded transparently)
draft-ietf-sip-connect-reuse-06	Connection Reuse in SIP	√	√
draft-ietf-sipping-cc-transfer-05	Call Transfer	√	√
draft-ietf-sipping-realtimefax-01	SIP Support for Real-time Fax: Call Flow Examples	√	√ (forwarded transparently)
draft-ietf-sip-privacy-04.txt	SIP Extensions for Network-Asserted Caller Identity using Remote-Party-ID header	√	√
draft-johnston-sipping-cc-uui-04	Transporting User to User Information for Call Centers using SIP	√	√ (forwarded transparently)
draft-levy-sip-diversion-08	Diversion Indication in SIP	√	√
draft-mahy-iptel-cpc-06	The Calling Party's Category tel URI Parameter	√	√ (forwarded transparently)
draft-mahy-sipping-signaled-digits-01	Signaled Telephony Events in the Session Initiation Protocol	√	√
draft-sandbakken-dispatch-bfcp-udp-03	Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport	×	√ (forwarded transparently)
ECMA-355, ISO/IEC 22535	QSIG tunneling	√	√ (forwarded transparently)
RFC 2327	SDP	√	√
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication	√	√
RFC 2782	A DNS RR for specifying the location of services	√	√
RFC 2833	Telephone event	√	√
RFC 2976	SIP INFO Method	√	√
RFC 3261	SIP	√	√
RFC 3262	Reliability of Provisional Responses	√	√

69

RFC	Description	Gateway	SBC
RFC 3263	Locating SIP Servers	√	√
RFC 3264	Offer/Answer Model	√	√
RFC 3265	(SIP)-Specific Event Notification	√	√
RFC 3310	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)	√	×
RFC 3311	UPDATE Method	√	√
RFC 3323	Privacy Mechanism	√	√
RFC 3325	Private Extensions to the SIP for Asserted Identity within Trusted Networks	√	√
RFC 3326	Reason header	√	√ (forwarded transparently)
RFC 3327	Extension Header Field for Registering Non-Adjacent Contacts	√	×
RFC 3361	DHCP Option for SIP Servers	√	×
RFC 3362	Real-time Facsimile (T.38) - image/t38 MIME Sub-type Registration	√	√
RFC 3372	SIP-T	√	√ (forwarded transparently)
RFC 3389	RTP Payload for Comfort Noise	√	√ (forwarded transparently)
RFC 3420	Internet Media Type message/sipfrag	√	√
RFC 3455	P-Associated-URI	√	√ (using user info \ account)
RFC 3489	STUN - Simple Traversal of UDP	√	√
RFC 3515	Refer Method	√	√
RFC 3550	RTP: A Transport Protocol for Real-Time Applications	√	√
RFC 3578	Interworking of ISDN overlap signalling to SIP	√	×
RFC 3581	Symmetric Response Routing - rport	√	√
RFC 3605	RTCP attribute in SDP	√	√ (forwarded transparently)
RFC 3608	SIP Extension Header Field for Service Route Discovery During Registration	√	×
RFC 3611	RTCP-XR	√	√
RFC 3665	SIP Basic Call Flow Examples	√	√
RFC 3666	SIP to PSTN Call Flows	√	√ (forwarded transparently)
RFC 3680	A SIP Event Package for Registration (IMS)	√	×
RFC 3711	The Secure Real-time Transport Protocol (SRTP)	√	√
RFC 3725	Third Party Call Control	√	√

RFC	Description	Gateway	SBC
RFC 3824	Using E.164 numbers with SIP (ENUM)	√	√
RFC 3842	MWI	√	√
RFC 3891	"Replaces" Header	√	√
RFC 3892	The SIP Referred-By Mechanism	√	√
RFC 3903	SIP Extension for Event State Publication	√	√
RFC 3911	The SIP Join Header	Partial	×
RFC 3960	Early Media and Ringing Tone Generation in SIP	Partial	√
RFC 3966	The tel URI for Telephone Numbers	√	√
RFC 4028	Session Timers in the Session Initiation Protocol	√	√
RFC 4040	RTP payload format for a 64 kbit/s transparent call - Clearmode	√	√ (forwarded transparently)
RFC 4117	Transcoding Services Invocation	√	×
RFC 4168	The Stream Control Transfer Protocol (SCTP) as a Transport for SIP	×	√
RFC 4235	Dialog Event Package	Partial	Partial
RFC 4240	Basic Network Media Services with SIP - NetAnn	√	√ (forwarded transparently)
RFC 4244	An Extension to SIP for Request History Information	√	√
RFC 4320	Actions Addressing Identified Issues with SIP Non-INVITE Transaction	√	√
RFC 4321	Problems Identified Associated with SIP Non-INVITE Transaction	√	√
RFC 4411	Extending SIP Reason Header for Preemption Events	√	√ (forwarded transparently)
RFC 4412	Communications Resource Priority for SIP	√	√ (forwarded transparently)
RFC 4458	SIP URIs for Applications such as Voicemail and Interactive Voice Response	√	√ (forwarded transparently)
RFC 4475	SIP Torture Test Messages	√	√
RFC 4497 or ISO/IEC 17343	Interworking between SIP and QSIG	√	√ (forwarded transparently)
RFC 4566	Session Description Protocol	√	√
RFC 4568	SDP Security Descriptions for Media Streams for SRTP	√	√
RFC 4582	The Binary Floor Control Protocol (BFCP)	×	√ (forwarded transparently)
RFC 4715	Interworking of ISDN Sub Address to sip isub parameter	√	√ (forwarded transparently)
RFC 4730	A SIP Event Package for Key Press Stimulus (KPML)	Partial	×
RFC 4733	RTP Payload for DTMF Digits	√	√

RFC	Description	Gateway	SBC
RFC 4904	Representing trunk groups in tel/sip URIs	√	√ (forwarded transparently)
RFC 4960	Stream Control Transmission Protocol	×	√
RFC 4961	Symmetric RTP and RTCP for NAT	√	√
RFC 4975	The Message Session Relay Protocol (MSRP)	×	√
RFC 5022	Media Server Control Markup Language (MSCML)	√	×
RFC 5079	Rejecting Anonymous Requests in SIP	√	√
RFC 5627	Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in SIP	√	√ (forwarded transparently)
RFC 5628	Registration Event Package Extension for GRUU	√	×
RFC 5806	Diversion Header, same as draft-levy-sip-diversion-08	√	√
RFC 5853	Requirements from SIP / SBC Deployments	-	√
RFC 6035	SIP Package for Voice Quality Reporting Event, using sip PUBLISH	√	√
RFC 6135	An Alternative Connection Model for the Message Session Relay Protocol (MSRP)	×	√
RFC 6140	Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)	√	√
RFC 6337	Session Initiation Protocol (SIP) Usage of the Offer/Answer Model	-	√
RFC 6341	Use Cases and Requirements for SIP-Based Media Recording (Session Recording Protocol - draft-ietf-siprec-protocol-02, and Architecture - draft-ietf-siprec-architecture-03)	√	√
RFC 6442	Location Conveyance for the Session Initiation Protocol	-	√
RFC 7245	An Architecture for Media Recording Using the Session Initiation Protocol	√	√
RFC 7261	Offer/Answer Considerations for G723 Annex A and G729 Annex B	√	√
RFC 7865	Session Initiation Protocol (SIP) Recording Metadata	√	√
RFC 7866	Session Recording Protocol	√	√
RFC 8068	Session Initiation Protocol (SIP) Recording Call Flows	√	√

4.2 SIP Message Compliancy

The SIP device complies with RFC 3261, as shown in the following subsections.

4.2.1 SIP Functions

The device supports the following SIP Functions:

Table 4-2: Supported SIP Functions

Function	Comments
User Agent Client (UAC)	-
User Agent Server (UAS)	-
Proxy Server	The device supports working with third-party Proxy Servers such as Nortel CS1K/CS2K, Avaya, Microsoft OCS, Alcatel, 3Com, BroadSoft, Snom, Cisco and many others
Redirect Server	The device supports working with third-party Redirection servers
Registrar Server	The device supports working with third-party Registration servers

4.2.2 SIP Methods

The device supports the following SIP Methods:

Table 4-3: Supported SIP Methods

Method	Comments
ACK	-
BYE	-
CANCEL	-
INFO	-
INVITE	-
MESSAGE	Supported only by the SBC application and send only
NOTIFY	-
OPTIONS	-
PRACK	-
PUBLISH	Send only
REFER	Inside and outside of a dialog
REGISTER	Send only for Gateway application; send and receive for SBC application
SUBSCRIBE	-
UPDATE	-

4.2.3 SIP Headers

The device supports the following SIP headers:

Table 4-4: Supported SIP Headers

SIP Header	SIP Header
Accept	Proxy- Authenticate
Accept–Encoding	Proxy- Authorization
Alert-Info	Proxy- Require
Allow	Prack
Also	Reason
Asserted-Identity	Record- Route
Authorization	Refer-To
Call-ID	Referred-By
Call-Info	Replaces
Contact	Require
Content-Disposition	Remote-Party-ID
Content-Encoding	Response- Key
Content-Length	Retry-After
Content-Type	Route
Cseq	Rseq
Date	Session-Expires
Diversion	Server
Expires	Service-Route
Fax	SIP-If-Match
From	Subject
History-Info	Supported
Join	Target-Dialog
Max-Forwards	Timestamp
Messages-Waiting	To
MIN-SE	Unsupported
P-Associated-URI	User- Agent
P-Asserted-Identity	Via
P-Charging-Vector	Voicemail
P-Preferred-Identity	Warning
Priority	WWW- Authenticate
Privacy	-

Note: The following SIP headers are not supported:

- **Encryption**
- **Organization**

4.2.4 SDP Fields

The device supports the following SDP fields:

Table 4-5: Supported SDP Fields

SDP Field	Name
v=	Protocol version number
o=	Owner/creator and session identifier
a=	Attribute information
c=	Connection information
d=	Digit
m=	Media name and transport address
s=	Session information
t=	Time alive header
b=	Bandwidth header
u=	URI description header
e=	Email address header
i=	Session info header
p=	Phone number header
y=	Year

4.2.5 SIP Responses

The device supports the following SIP responses:

Table 4-6: Supported SIP Responses

Response Type		Comments
1xx Response (Information Responses)		
100	Trying	The device generates this response upon receiving a Proceeding message from ISDN or immediately after placing a call for CAS signaling.
180	Ringing	The device generates this response for an incoming INVITE message. Upon receiving this response, the device waits for a 200 OK response.
181	Call is Being Forwarded	The device doesn't generate these responses. However, the device does receive them. The device processes these responses the same way that it processes the 100 Trying response.
182	Queued	The device generates this response in Call Waiting service. When the SIP device receives a 182 response, it plays a special waiting Ringback tone to the telephone side.
183	Session Progress	The device generates this response if the Early Media feature is enabled and if the device plays a Ringback tone to IP
2xx Response (Successful Responses)		
200	OK	

Response Type		Comments
202	Accepted	
204	No Notification	
3xx Response (Redirection Responses)		
300	Multiple Choice	The device responds with an ACK, and then resends the request to the first new address in the contact list.
301	Moved Permanently	The device responds with an ACK, and then resends the request to the new address.
302	Moved Temporarily	The device generates this response when call forward is used to redirect the call to another destination. If such a response is received, the calling device initiates an INVITE message to the new destination.
305	Use Proxy	The device responds with an ACK, and then resends the request to a new address.
380	Alternate Service	The device responds with an ACK, and then resends the request to a new address.
4xx Response (Client Failure Responses)		
400	Bad Request	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
401	Unauthorized	Authentication support for Basic and Digest. Upon receipt of this message, the device issues a new request according to the scheme received on this response.
402	Payment Required	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
403	Forbidden	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
404	Not Found	The device generates this response if it is unable to locate the callee. Upon receiving this response, the device notifies the User with a Reorder Tone.
405	Method Not Allowed	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
406	Not Acceptable	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
407	Proxy Authentication Required	Authentication support for Basic and Digest. Upon receipt of this message, the device issues a new request according to the scheme received on this response.
408	Request Timeout	The device generates this response if the no-answer timer expires. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
409	Conflict	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.

Response Type		Comments
410	Gone	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
411	Length Required	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
413	Request Entity Too Large	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
415	Unsupported Media	If the device receives a 415 Unsupported Media response, it notifies the User with a Reorder Tone. The device generates this response in case of SDP mismatch.
420	Bad Extension	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
423	Interval Too Brief	The device does not generate this response. Upon receipt of this message the device uses the value received in the Min-Expires header as the registration time.
424	Bad Location Information	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
428	Use Identity Header	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
429	Provide Referrer Identity	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
433	Anonymity Disallowed	If the device receives a 433 Anonymity Disallowed, it sends a DISCONNECT message to the PSTN with a cause value of 21 (Call Rejected). In addition, the device can be configured, using the Release Reason Mapping, to generate a 433 response when any cause is received from the PSTN side.
436	Bad Identity Info	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
437	Unsupported Credential	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
438	Invalid Identity Header	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
439	First Hop Lacks Outbound Support	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
440	Max-Breadth Exceeded	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.

71

Response Type		Comments
470	Consent Needed	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
480	Temporarily Unavailable	If the device receives this response, it notifies the User with a Reorder Tone. This response is issued if there is no response from remote.
481	Call Leg/Transaction Does Not Exist	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
482	Loop Detected	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
483	Too Many Hops	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
484	Address Incomplete	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
485	Ambiguous	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
486	Busy Here	The SIP device generates this response if the called party is off-hook and the call cannot be presented as a call waiting call. Upon receipt of this response, the device notifies the User and generates a busy tone.
487	Request Canceled	This response indicates that the initial request is terminated with a BYE or CANCEL request.
488	Not Acceptable	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
491	Request Pending	When acting as a UAS: the device sent a re-INVITE on an established session and is still in progress. If it receives a re-INVITE on the same dialog, it returns this response to the received INVITE. When acting as a UAC: If the device receives this response to a re-INVITE, it starts a timer. After the timer expires, the UAC tries to send the re-INVITE again.
5xx Response (Server Failure Responses)		
500	Internal Server Error	Upon receipt of any of these responses, the device releases the call, sending an appropriate release cause to the PSTN side. The device generates a 5xx response according to the PSTN release cause coming from the PSTN.
501	Not Implemented	
502	Bad gateway	
503	Service Unavailable	
504	Gateway Timeout	

Response Type		Comments
505	Version Not Supported	
6xx Response (Global Responses)		
600	Busy Everywhere	Upon receipt of any of these responses, the device releases the call, sending an appropriate release cause to the PSTN side.
603	Decline	
604	Does Not Exist Anywhere	
606	Not Acceptable	

Consumption models evolve

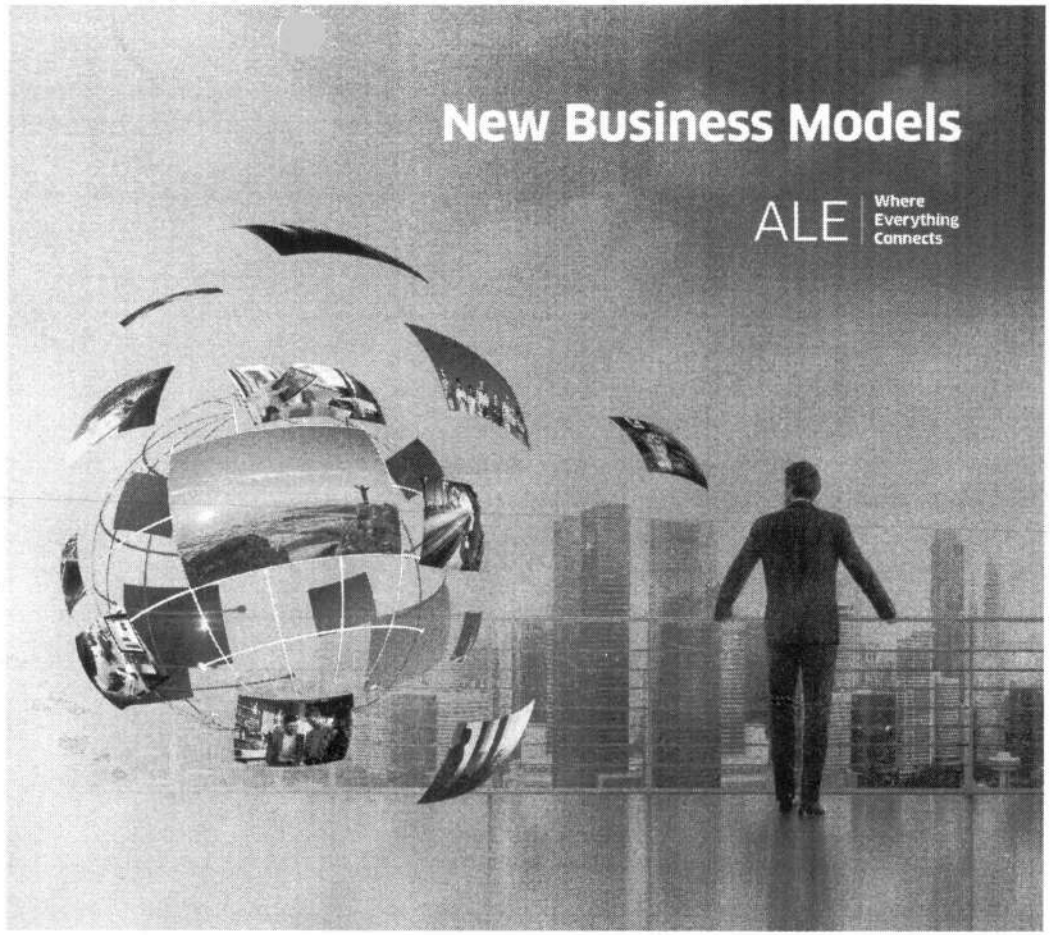
Before the advent of the electric utility grid, early electricity users owned, operated and maintained all the tools and hardware themselves. For those that could afford it, the cost of ownership was very high, distribution distance was low, and a seemingly random set of standards powered new uses from lighting to industrial motors.

However, the innovation of early grids rapidly led to new innovations in electricity distribution and widespread adoption, enabling customers to draw from the grid only when they needed electricity.

Of course, this evolution did not occur without the active resistance of local power suppliers, who had enjoyed a healthy ROI selling into an increasingly dependent and closed market.

Although paying for electricity as a consumption-based service seems obvious to us now, the impact and benefits of metered on-demand electricity were not always universally accepted.

Alcatel·Lucent Enterprise



Changing the way businesses buy technology

Organizations have reached a complex and transformative stage in digital business as the pace of innovation accelerates every day. Technology purchased today will be two or three generations out of date by the time the book value is fully depreciated. Yet, that same technology is expected to contend with growing demands.

Alcatel·Lucent Enterprise

Technology models are evolving, aligning cost to revenue and business activity cycles.

Alcatel-Lucent Enterprise consumption models

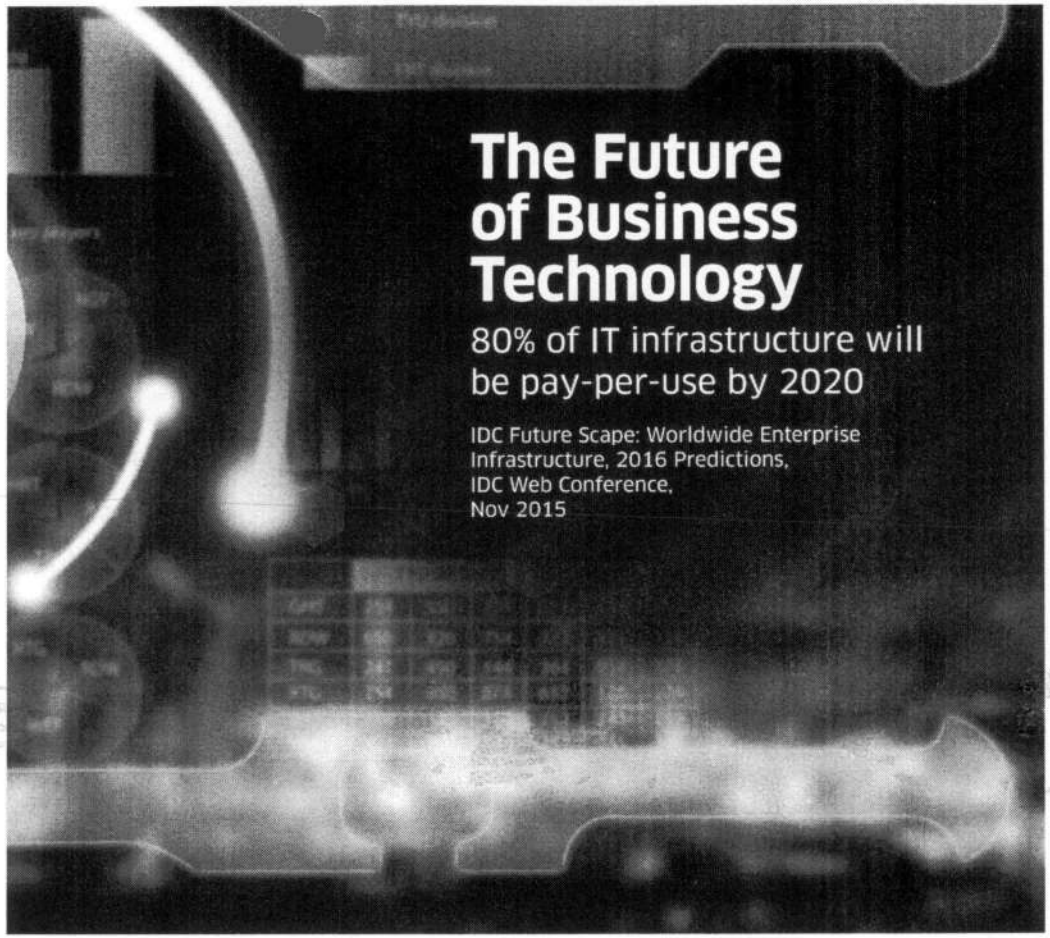
FREE YOUR CAPITAL To invest in your core business	PAY FOR WHAT YOU USE Adapt costs to business activity	BUSINESS AGILITY Rapid scalability	RISK SHARING True partnership
PAY PER OUTCOME (aligned to business)			
●	●	●	●
PAY PER USE (consumption)			
●	●	●	●
PAY PER MONTH (lease)			
●	●	●	●
PAY UPFRONT (capital)			
●	●	●	●

Total cost of Ownership (TCO)

Again overlooked, or at least under-defined, each is an alternative to the traditional B2B CAPEX model of "make, sell, ship," moving the relationship between vendor and customer towards a partnership based on mutual success.

Price and cost of ownership are not the same as any economist will explain, and business assessment considers factors beyond direct ownership costs.

In essence, while the acquisition cost of capital is tangible, and operational costs can be estimated, opportunity costs are often overlooked in cost analysis of technology capital investment.



Consume or Buy

Technology has long been a capital expense investment with a business value that often resembles a bell-curve over the period of functional life.

As new technologies are introduced in a CAPEX model, complexity and management costs also increase, in turn affecting the total cost of ownership.

In contrast, consumption models are scalable and outcome focused. The burden of managing complexity lies with the vendor.

But the strategic consideration of consumption models is not just about price. Price and cost of ownership are not the same.

While the acquisition capital cost is tangible, and operational costs can be estimated, opportunity costs are often overlooked in the cost analysis of technology capital investment.

Not all consumption models are equal and there is a relevant distinction between cloud, consumption, and outcome based models.

Portfolio of Services

Network on Demand is a new LAN and WiFi network infrastructure service built upon the pay-per-use concept where end customers only pay for network resources consumed – per connected port per day.

Network on Demand is built upon our existing portfolio of network technology and each Network on Demand deployment is tailored and scaled to the requirements of the end-user organization, based on their unique needs. Network on Demand enables flexibility for both customer and partner.

The unique and innovative feature of Network on Demand is the flexibility built in for the customers throughout the model.

At the end of the subscription period, customers can choose to refresh the necessary equipment and renew the subscription without a capex outlay, can pay off any remaining balance, or can simply end the relationship without penalty.

For many organizations, this will lower barriers to upgrading their networks to support digital transformation.

Open Touch Enterprise Cloud delivers a full featured enterprise communication service that is pay as you use, and fully managed for you. It offers a complete and secure solution delivering business telephony, unified communications, contact center, and industry specific services.

It can be deployed in any scenario including pure IP or TDM-based infrastructure, in a private cloud (off or on-premises), or in an overlay installation.

Open Touch Entreprise Cloud can align to business demands with a predictable cost that matches spending with use. The flexible 'consumption-based' licensing model makes it easy to scale up or down depending on changing requirements.

Rainbow is an overlay cloud service operated by us that enables cross-community interactions and transactions between business users that goes beyond traditional company borders.

Rainbow offers contact management, presence, persistent messaging, audio and video calls, screen and file sharing with PSTN termination and with seamless integration into existing ICT assets.

Rainbow proposes two service plans: Rainbow Essential and Rainbow Enterprise where each user is associated to a service plan whilst you can mix Essential & Enterprise service plans within the same company.

Optional services can be added to Rainbow Essential and Rainbow Enterprise for traffic-based services.

How it works

New business models verticalization

Our new business models strategy addresses each vertical market and delivers a commercial offer that aligns directly to unique business scenarios and outcomes.

Unique Integrated Cloud

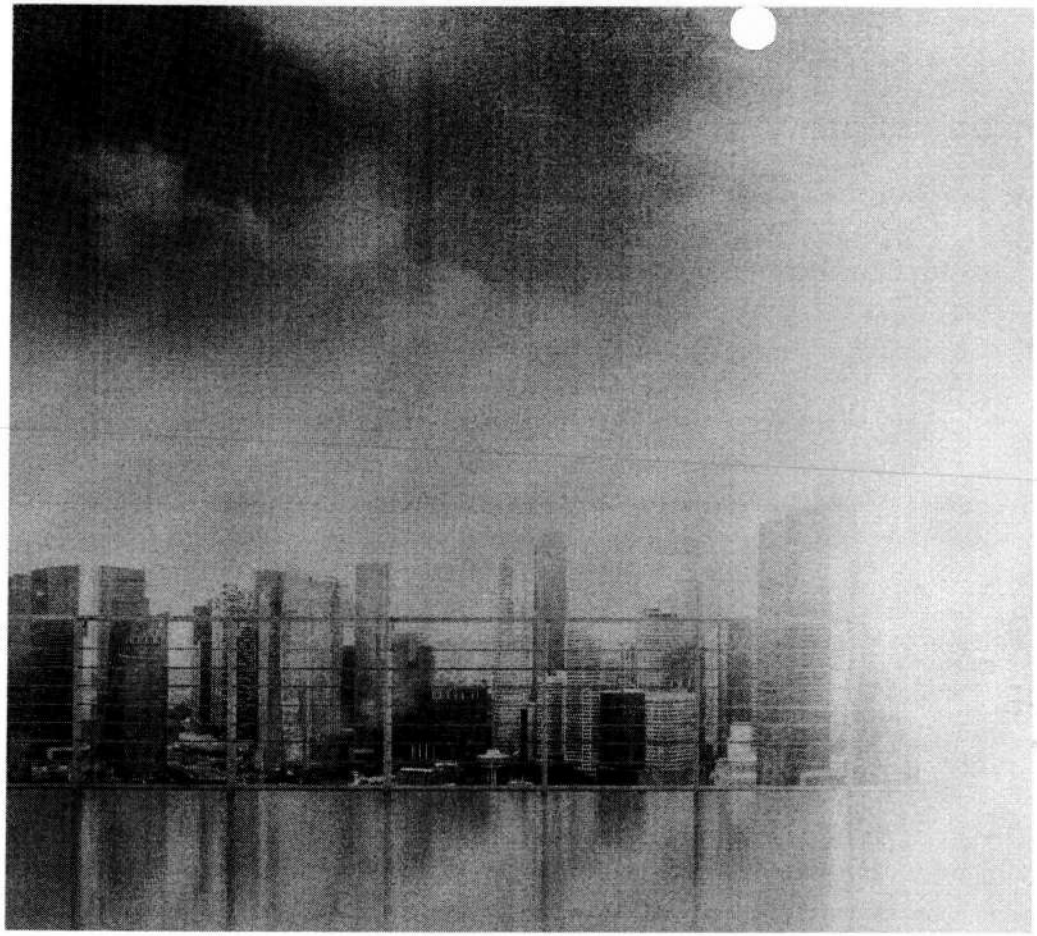
Our Integrated Cloud is made up of the blend of individual Services and the innovative commercial models suited to fit each customer needs.

What differentiates us is how we are changing the way businesses buy technology: how they deploy it, use it and leverage it.

By tailoring our partnership models to organisations and their people, processes and customers, organizations are able to configure and enable technology services, much like electricity is consumed today.

TCO Comparison matrix

	CAPEX / ON-PREMISE	AS A SERVICE / CLOUD
Hardware purchase	+	-
Software purchase	+	-
Implementation services	+	-
TOTAL CAPITAL EXPENDITURE	HIGHER	LOWER
Depreciation expense	+	-
Time value of money	+	-
Investment risk	+	-
Hardware/Software updates	+	-
Support and maintenance	+	-
As a Service	Pay per use only	Higher
Capacity overhead	Typically >10%	Pay per use / Unlimited
TOTAL OPERATING EXPENDITURE	Fixed	Adaptive



SERVICE LINE	SERVICE LINE COMPONENT	PRICE
Networking	Basic user port	Per connected service / business outcome
	Advanced user port	
	Server port	
	Uplink Port	
	Basic wireless access	
	Advanced wireless access	
Communications	Basic user	
	Mobile user	
	Advanced user	
	Switchboard	
	Call centre agent	
	Call centre supervisor	
	SIP trunks	
	Redundancy	

A new breed of partnership

We have initiatives that align with the desire to purchase technology for business reasons, not technology reasons.

We make everything connect by delivering networking and communications technology that works for you.

Together with our business partners we are delivering business outcomes that are focused on tailoring solutions to the people, processes and customers of your business.

Our partnership strategy is one of shared technology opportunity and risk, aligned with our vision to ultimately change the way customers buy technology.

With Alcatel-Lucent Enterprise you can provision your network, communications infrastructure and applications as a Service and benefit by:

- **Freeing up working capital for core business activities and reducing over-capitalization on technology;**
- **Aligning costs directly with business activity providing customers with a more adaptive cost and the ability to quickly scale both up and down;**
- **Leveraging existing technology investments and creating a true risk sharing arrangement.**

Document number:
Date:
Copyright:

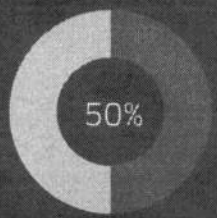
Reallocate funds for an innovative and competitive advantage

Compelling cost and business benefits

The ongoing digital transformation of the enterprise requires key elements to be addressed including operational agility, the customer experience and the integration of digital technology. Digital transformation also requires many things including an infrastructure that aligns with business growth, a way to provide employees the right services wherever they are, and the means to deliver frequent updates and upgrades to the communications system. This digital transformation environment has elevated the importance of cloud services.

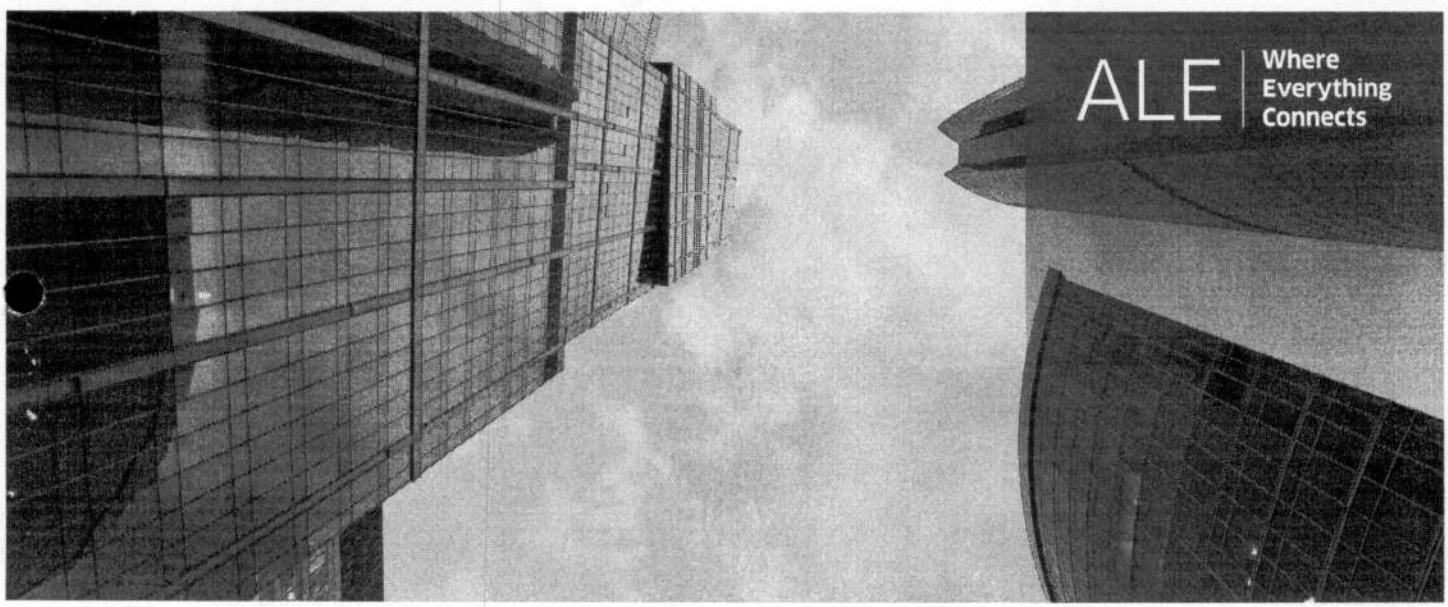
The cloud is attracting more and more businesses. The majority of early adopters are small- and medium-sized businesses (SMBs), which is consistent with their desire for lower upfront costs, flexibility and ease of deployment in that particular market segment. However, enterprises with an extensive footprint or multi-branch office topologies are also increasingly adopting cloud-based offerings as they seek to, more effectively, support global operations and a growing number of remote and mobile workers.

Therefore, there are many reasons for organizations to move from traditional IT infrastructures to cloud-based infrastructures. One of the most cited reasons is the financial aspect of the cloud, with its compelling cost and business benefits.



By 2018, at least half of IT spending will be cloud-based.*

Source: IDC FutureScape: Worldwide Cloud 2016 Predictions



OpenTouch Enterprise Cloud

Cloud economics

76

Brochure
OpenTouch Enterprise Cloud
July 2017

Alcatel·Lucent Enterprise

Shift from CAPEX to OPEX

Moving from a CAPEX to an OPEX business model allows enterprises to manage operational expenses rather than capital assets, and focus on operating statements rather than balance sheet management. OpenTouch Enterprise Cloud offers a 100% OPEX business model. This is ideal for companies looking for consumption-based models and that want to replace their existing CAPEX model.

Minimum or zero upfront investment

A cloud business model can reduce or eliminate the investment required to launch new projects and lets businesses re-align cash flow requirements with solution adoption, over time. Freed from the risks associated with upfront investments, IT departments can focus on value-added activities that promote the business.

Overcome expenditure limitations

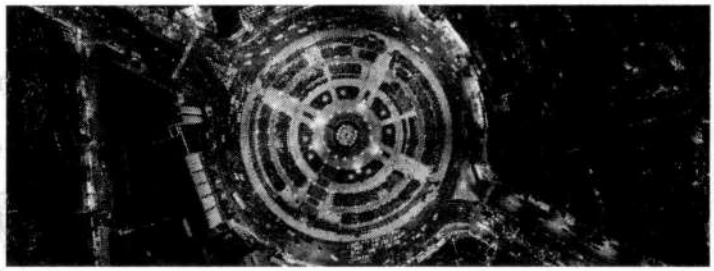
While obtaining capital for large purchases may be difficult for any size of organization, it is especially difficult for smaller organizations where rigorous debt to equity ratios are applied and can restrict the amount of capital a company can secure. This makes it difficult for organizations to sufficiently justify capital expenditure and get approval for projects. Moving to an OPEX model removes the financial scrutiny and allows projects to be undertaken, unconstrained by capital considerations.

Flexibility to terminate costs as required

An OPEX business model provides organizations with the flexibility to terminate costs to match business demands. With a CAPEX business model, acquiring a server or software requires a full financial commitment. Regardless of whether it is being used, the ongoing costs (depreciation or financing costs) still need to be managed. Contrast this with the OPEX business model where payments can rapidly cease if the item is no longer required.

Transparent costs - ease forecasting

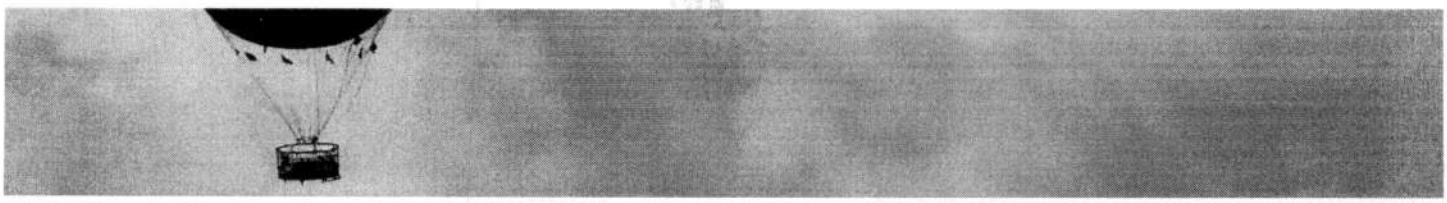
Costs associated with cloud-based systems are considerably more transparent than on-premise systems. Studies show, when it comes to cloud software, that most of the costs (approximately 70%) will be encountered in the form of monthly subscriptions.



With on-premise solutions, only the cost of software licenses is known in advance, which accounts for less than 10% of the costs. Most of the costs with on-premise solutions are associated with customization, implementation, hardware, IT personnel, maintenance and training. With cloud-based software, unexpected costs primarily relate to implementation, customization and training, which makes costs a lot more transparent and easier to forecast.

Tax deductible - balance sheet not affected

From a pure financial perspective, CAPEX items require a major investment in goods, which are accounted for on the balance sheet and are depreciated over the life of the goods. OPEX items, on the other hand, are accounted for on the P&L (Profit and Loss statement) which tracks ongoing expenses as they are incurred and doesn't affect the balance sheet. One final important consideration is that in most countries, OPEX is tax deductible and CAPEX is not.

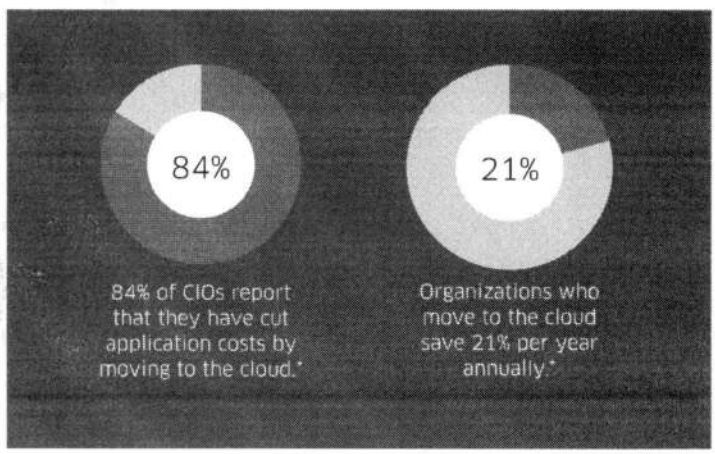


Five financial reasons why enterprises move to cloud-based solutions

Many business owners believe that the cost advantage of cloud-based solutions is one of the most important benefits. Below are five important financial benefits:

1. The ability to shift from capital expenditures (CAPEX) to operational expenditures (OPEX)
2. A pay-as-you-go business model
3. Greater financial agility
4. Reduced IT (Information Technology) costs
5. Service delivery time savings

Let's take a deeper look at these five points and see how Alcatel-Lucent OpenTouch* Enterprise Cloud can help businesses streamline operations and save money.



*Source: The State of the Cloud 2015 - Supply Chain Adopters Reaping ROI Rewards

“ This agility can give businesses, opting for cloud-based solutions, a real advantage over competitors. ”

Greater financial agility

High flexibility

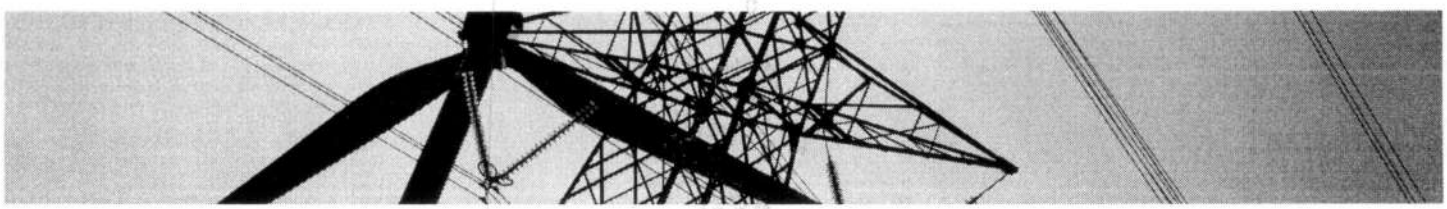
Cloud-based services are ideal for businesses with growing or fluctuating bandwidth demands. If needs increase it's easy to scale up the cloud capacity. And, if the business needs to scale down again, the flexibility is available to reduce the service.

Additionally, the up-front cost of a cloud solution is lower (or can even be eliminated) than an on-premise solution. For companies that need top-tier products but don't have extensive funds immediately available, cloud solutions offer a high degree of flexibility.

This agility can give businesses, opting for cloud-based solutions, a real advantage over competitors.

OpenTouch Enterprise Cloud is a financially feasible solution that can be fine tuned on demand, scaling up or down according to business needs. For example, if the customer and project demands require increased teamwork, collaboration tools can quickly be accessed without advanced planning and without spending extra money for additional hardware or software. Likewise, expenses can quickly be reduced if demand for services is reduced.

No increased hardware and software costs when demand for service is increased



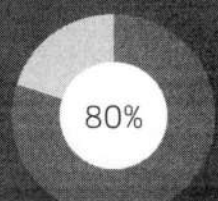
Pay-as-you-grow

Pay for what you use

Cloud-based solutions lead to a more predictable cost model and allow organizations to only pay for what they need, and for what they use, on a monthly basis. No more multi-year contracts, no more daunting up-front fees. Just simple, accessible technology, paid for in a simple, accessible way. Ultimately, this allows organizations to streamline applications and save money. Think of it when using electricity for example: Your consumption rate is based on what you actually use and no more.

OpenTouch Enterprise Cloud provides payment flexibility and avoids unnecessary over provisioning of capacity. This means:

- Companies don't pay for wasted resources, since users are only charged for the services procured, rather than provisioning for a certain amount of resources that will not be used
- Services can be cancelled at any time, without any fees, when they are no longer required



By 2020, more than 80% of software vendors will change their business models from traditional license and maintenance to subscription.*

*Source: Moving to a Software Subscription Model, Gartner report, 2015

78

Service delivery time savings

Accelerated delivery of services and applications

Each time an organization wants to add a new service, it requires a significant investment in time, staff, training and money. The cloud business model:

- Improves the agility of company services, since the deployment of cloud software is faster than a conventional installation.
- Offers service delivery time savings because virtualization and service management software help automate the service delivery process. This is one of the biggest cost saving areas, with some organizations experiencing up to 70 percent reduction in service delivery time.

OpenTouch Enterprise Cloud communication applications for fast business response can be deployed in a matter of hours, ensuring communication quality between employees and customers are improved almost immediately. And because cloud-based applications are available anywhere there is internet access, all employees on the go, in virtual offices and remote sites are immediately more productive. In addition, communications with colleagues becomes free.

Shared services

With cloud-based solutions, services can be shared across multiple locations of a company creating a catalyst for business process simplification and standardization, and providing further cost saving opportunities.

IT cost savings

Few technologies have affected the IT industry as profoundly as cloud computing. Cloud computing allows organizations to shed at least some of their expensive IT infrastructure and shift costs to more manageable operational expenses.

Eliminate the risk of technology obsolescence

The amount of IT staff time required to support IT environments increases as equipment ages. As equipment gets older, it's more likely to fail and it becomes more challenging to patch and update. As a result, the cost of supporting aging equipment can quickly escalate. These creeping costs can be challenging for organizations to identify and manage effectively. Cloud-based solutions eliminate the risks associated with technology obsolescence.

Minimize disruptions

Application and system outages can also impact costs in terms of lost productivity and revenue leakage. An IT environment with minimal disruptions is the ultimate goal for cost effective business operations. Cloud-based solutions can help reduce costs associated with outages. With cloud-based solutions organizations can leverage the expertise of vendors and partners to architect and deploy solutions, which lead to the reduced frequency and duration of outages.

Eliminate system redundancy expenditures

When organizations transition to cloud infrastructures they no longer have to worry about buying additional hardware to ensure redundancy for reliable business continuity. Typical cloud solutions have several data center locations that mirror data and applications across at least two locations. It's a less expensive way to ensure redundancy, and is just another benefit of the economies of scale delivered by the cloud.

Reduce maintenance costs and IT personnel

It's acknowledged, industry-wide, that IT maintenance accounts for approximately 80% of total IT expenditures. Cloud-based solutions require less in-house IT staff as a result of systems being owned and stored by vendors in their off-site locations

resulting in significant labor and maintenance savings. When systems require repairs or upgrades, it is the responsibility of the vendor. For companies lacking the resources for in-house IT staff, cloud-based solutions can help eliminate costly IT expenditures.

Spend more time on core business processes - free up cash

Instead of wasting time on processes that don't create value for the organization (such as refreshes and upgrades of equipment and systems, and backups), cloud-based solutions let IT departments focus on core business processes which can free up cash to invest, for example, in business applications.

The amount of money IT will spend on cloud services this year is $114 billion, and will grow to $216 billion by the year 2020.*

With OpenTouch Enterprise Cloud, businesses invest in services that meet the demands of the workforce by making unified communications (UC), conferencing and mobility, available to all employees without requiring extensive training and increasing the IT staff workload.

79

*Source: Gartner 2017 Predicts 2016

Reallocate money to innovate
and grow the business

Choose Alcatel-Lucent
OpenTouch Enterprise Cloud

Alcatel·Lucent
Enterprise

Green savings

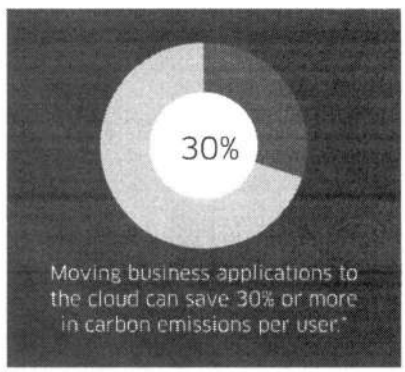
Even if the cost benefit of the green business case is not top of mind for business owners, this growing trend cannot be ignored.

As the cloud continues to grow and evolve, new trends will continue to emerge. Notably the sustainability of cloud computing. Migrating to the cloud means fewer machines and less hardware, which translates into reduced cooling and space requirements. The end results are lower energy costs and freed up capital that companies can allocate for other opportunities.

The cloud offers companies the ability to reduce their carbon footprint and move toward a greener, smarter future. Undoubtedly, cloud adoption and improved efficiencies will become increasingly ubiquitous with advancements in cloud technology and growing green awareness.

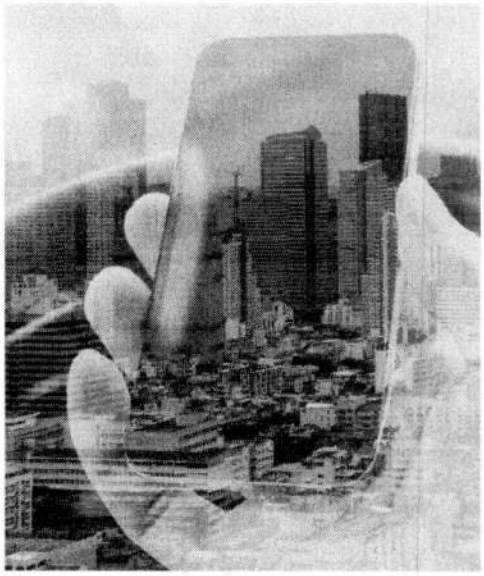
Here are few reasons why OpenTouch Enterprise Cloud is a smart green investment:

- Less on-premise hardware
- Efficient use of server resources
- Shared infrastructures operate more efficiently and consume less power



Source: Study conducted by Accenture and WSP Environment & Energy, 2012

90



Alcatel-Lucent OpenTouch Enterprise Cloud

Boost enterprise productivity and agility, and improve your bottom line with communications delivered from the Cloud

Enterprises are being asked to address increasing communication demands while stretching their dollars further. They need a creative solution to address employee demands, improve productivity, and reduce their Total Cost of Ownership (TCO). The answer – the Cloud.

COMMUNICATION TRENDS

The traditional workplace – where employees commute to a fixed location for a set length of time during business hours – is disappearing. Workers now expect to use the same devices and applications at home and at work, and have their IT department support them seamlessly.

Communications delivered from a Cloud Service Provider let enterprise employees use their devices to share documents and applications, participate in virtual meetings and conferences, and access all-inclusive applications and services anywhere, anytime. Additionally, businesses can enjoy the benefits of improved agility, enabling them to respond to rapidly changing business demands. They can also manage costs and focus on growing their core business.

TACKLE THE CHALLENGES

Businesses or technologies that are a "sure thing" today may be forgotten or surpassed tomorrow. Enterprises need to anticipate the rapid shifts in their business environment and adapt quickly to scale up to support new technologies or new resources, and scale back in other areas as required.

A Cloud Service Provider can help enterprises achieve their business objectives. Resources can be added or removed almost instantaneously, and they can be accessed from almost every location and device. A cloud architecture can offer advanced security and redundancy features and can significantly reduce the enterprise's TCO.

81

Alcatel·Lucent
Enterprise

DELIVER POWERFUL SOLUTIONS

AN END-TO-END COMMUNICATIONS SOLUTION

From small- to large-sized enterprises, OpenTouch® Enterprise Cloud delivers unprecedented openness across technologies, applications and platforms. It can be deployed in any scenario including, pure IP or TDM-based infrastructure, in a private cloud, or in an overlay installation, as a migration to a new platform, or as an upgrade to existing technology.

A SCALABLE AND RELIABLE CONTACT CENTER SOLUTION

OpenTouch Enterprise Cloud includes the Alcatel-Lucent OmniTouch® Contact Center Standard Edition. This solution is ideal for contact centers with up to 5000 agents. The fully packaged solution includes supervision, call distribution, interactive voice response, desktop agent and outbound calling features. As well it includes enhanced wallboard features that allow enterprises to customize functionality according to their specific requirements to enhance productivity and increase customer satisfaction. As for Unified Communications, this complete contact center solution is also available as a service (CCaaS).

REAP THE BENEFITS

BOOST PRODUCTIVITY

The new workplace is a mix of open spaces, huddle rooms, remote workers, and highly mobile users. It demands borderless interactions between employees, enterprise customers, and partners. OpenTouch Enterprise Cloud, based on the award winning OpenTouch Suite for MLE, lets enterprises optimize their communications and benefit from improved productivity.

With cloud-based, a-la-carte options, Cloud Service Providers can offer communications and collaboration that best suit the enterprise user's preferences or context. This includes deskphones and computers, mobile phones and tablets, and video conferencing. At the heart of the user-focused experience is the OpenTouch Conversation® Client, which enables enterprise employees to communicate with maximum efficiency and effectiveness.

INCREASE AGILITY

Adapting to rapidly changing business demands is key to success. OpenTouch Enterprise Cloud can adjust on the fly to meet the needs of any organization. New capabilities or increased capacity can be added in the network, without requiring additional hardware to be installed on site.

Cloud-based communications ensures the quick execution of Move-Add-Change-Delete operations. Depending on the Cloud Service Provider, enterprises can self-manage through their WebPortal to address these daily operations. Capacity can also be increased or decreased any time, to respond to business changes and dynamics.

GROW YOUR BOTTOM LINE AND THEIRS

Cloud-based delivery ensures organizations are always running the latest software, and it eliminates maintenance and upgrade costs. It lets enterprises reduce their capital outlay, and re-assign resources to focus on growing their business. It is a true 'pay-as-you-grow' solution.

Cloud Service Providers and enterprises also benefit from elastic licensing models. With OpenTouch Enterprise Cloud, organizations pay for services that are actually consumed. This enables enterprises to better align their costs with their requirements, for example in the hospitality industry where usage fluctuates depending on occupancy rates. Elastic licensing models also create an opportunity for Cloud Service Providers to grow their bottom line as service consumption increases.

IT'S TIME FOR THE CLOUD

With OpenTouch Enterprise Cloud organizations can boost productivity, address dynamic business demands, and improve collaboration with rich, context-based information anywhwere, from any device. It's time to move to the Cloud.

Alcatel-Lucent Enterprise solutions and services are available on-premise or from the cloud, and are marketed under the Alcatel-Lucent Enterprise brand. From the smallest startup to the largest multinational Alcatel-Lucent Enterprise solutions help enterprises benefit from a secure, high-performing communications infrastructure.

enterprise.alcatel-lucent.com

Alcatel·Lucent Enterprise

82

Alcatel·Lucent
Enterprise

Alcatel-Lucent OmniPCX Enterprise Communication Server

The expert enterprise phone system for medium, large and very large-sized companies

Alcatel-Lucent OmniPCX® Enterprise Communication Server (CS) offers business communications designed for the digital age. It connects the entire enterprise and provides organisations the freedom, quality, and agility they need to grow their business.

OmniPCX Enterprise CS Purple is the next generation of business communications solution, featuring advanced and flexible calls management, multimedia conversations, cloud openness and hybrid cloud connectivity with Rainbow™ by Alcatel-Lucent Enterprise to integrate mobility, video conferencing, and secure group messaging into your business applications.

Features	Benefits
Excellent voice connectivity to customers and employees	Quality business response: Zero lost calls; powerful com-munication tools ensure instant connection to the right people
Ensure employees can call wherever they are, on any device	Mobility: Standardized communication experience across the organization; employees can use desk phones, wire-less handsets, or softphones at the office, on site, at home or on the move
A borderless and mobile collaboration application lets employee connect the phone system to the Alcatel-Lucent Rainbow cloud-based unified communications service	Instant business response: Employees exchange instant messages, video, and screen sharing with their teams and business community while leveraging the office phone Simplicity: Unified communications delivered by a cloud service connected to the phone system; seamless user experience; agile IT operations
Serve users across multiple sites, with guaranteed high availability	Cost-saving: Expect lower telecom bills with free Voice over IP (VoIP) across sites, built-in least-cost routing and centralized trunks to SIP, and traditional service providers Reliability: High-availability options maintain vital business continuity during network or server outages

83

Technical specifications

Premium Business Communications

User experience

- Centralized directory with call by name
- Multi-line telephony
- Call options, including speed dial
- Audio conferencing
- Personal and enterprise call routing and forwarding
- Call shift of current session between desk phone and mobile device of choice
- Call-back and call history features
- Messaging notification and control
- Contextual voice prompts
- Informal group features
- Desk-sharing for shared offices
  - ALE Enterprise and Essential DeskPhones (IP)
  - Alcatel-Lucent Premium DeskPhones (IP)
  - Logon, logoff, re-logon
  - Automatic logoff

Manager/assistant

- Teams
- Filtered lines and private lines
- Text messaging, IM and voice messaging
- Discreet listening

Teams and groups

- Hunting groups and queues
- Supervision

Multi-tenancy

- Services per entity:
  - Speed dial
  - CLIP/CLIR
  - Auto attendant
  - Greeting message
  - Music on hold
  - Night service

Supported phones:

- Alcatel-Lucent New Office Environment (NOE) protocol
  - ALE Enterprise ALE-300, ALE-400, ALE-500 DeskPhones (IP)
  - ALE Essential ALE-20h, ALE-30h DeskPhones (IP/digital)
  - ALE Essential ALE-20 DeskPhone (IP)
  - Alcatel-Lucent 8008 (G) (CE), 8018 Deskphones (IP)
  - Alcatel-Lucent 8028s, 8058s, 8068s, 8078s Premium DeskPhones (IP)
  - Alcatel-Lucent 8029s, 8039s Premium DeskPhones (digital)
  - Alcatel-Lucent IP Desktop Softphone
  - Alcatel-Lucent 8158s, 8168s WLAN Handsets
- Alcatel-Lucent 8232 8242, 8234, 8244, 8254, 8262, 8262EX DECT handsets

Essential Business Communications

User experience

- Multi-line telephony
- Personal call forwarding
- Informal group features
- Message waiting indication
- Computer Telephony Integration (CTI)
- Supervision

Supported phones

- Session Initiation Protocol (SIP)
  - ALE SoftPhone
  - Alcatel-Lucent 8088 Smart DeskPhone
  - Alcatel-Lucent 8028s Premium DeskPhone
  - ALE-2, 8008 (G) (CE), 8018 DeskPhones
  - Alcatel-Lucent 8135s IP Conference Phone
- Third-party SIP phones and softphones
  - Developer and Solutions Partner Program (DSPP)

Huddle video rooms

- Session Initiation Protocol (SIP)
- Peer-to-peer video
- Join a video conference
  - Alcatel-Lucent OpenTouch® Multimedia Services
  - Third-party video room systems (DSPP)
- Supported phones
  - 8088 Smart DeskPhone

Unified Communications and Collaboration

Enterprise mobility, desktop integration, enterprise instant messaging

- Cloud-based UC&C:
  - Alcatel-Lucent Rainbow cloud connectivity
  - Alcatel-Lucent Rainbow user experience
  - See on-the-phone presence status
  - Search directory and click to call from desk phone or cordless handset
  - Pop-up notification when phone rings
  - Communication history
  - Call to/from Rainbow client (WebRTC Gateway)
  - One number service: desk phone, Rainbow smartphone and desktop apps
- Premise-based UC&C:
  - OpenTouch Multimedia Services
  - Alcatel-Lucent OpenTouch Conversation user experience

Messaging

- Integrated voice messaging:
  - Alcatel-Lucent 4645 Voice Messaging Service
- Unified messaging and fax:
  - OpenTouch Multimedia Services
- Centralized voice messaging:
  - Alcatel-Lucent OpenTouch Message Center
- Centralized fax management:
  - Alcatel-Lucent OpenTouch Fax Center
- Third-party SIP voice messaging: DSPP

Web conferencing

- Cloud-based conferencing:
  - Alcatel-Lucent Rainbow cloud connectivity
- Premise-based conferencing:
  - OpenTouch Multimedia Services

Customer welcome and Contact center

Greeting services

- Call queuing services
- Alarm indication
- Attendant group features
- Busy Lamp Field
- Multi-tenant services
- Record online
- Trunk and charging features
- VIP line features
- User management features
- Add-on module
- Headset capability

Attendants

- Centralized attendant console
  - Alcatel-Lucent 4059EE Attendant Console

84

- Attendant contextual menus
  - ALE-300 or Alcatel-Lucent 8058s, 8068s, 8078s Premium DeskPhones
- Automated Attendant application:
  - Alcatel-Lucent Visual Automated Attendant (VAA)

Voice announcement

- External/Internal voices guides
  - From ALE DeskPhones
  - From audio file in Supervision Desktop
- Interactive Voice Response:
  - Alcatel-Lucent 4625 Interactive Voice Response (IVR)

Customer welcome and contact center

- Alcatel-Lucent OmniTouch Contact Center Standard Edition:
  - Built-in OmniPCX Enterprise call distribution
  - Distributed distribution over ABC network
  - Agent context menus: ALE Enterprise and Essential DeskPhones, 8008, 8018, 8019s DeskPhone, 8028s, 8029s, 8068s, 8078s Premium DeskPhones, IP Desktop Softphone
  - Supervision desktop application
  - Reports
  - Alcatel-Lucent OpenTouch Customer Service on-premises add-on
  - ALE Connect for omnichannel hybrid cloud services and web-based agent/supervisor desktop application

Recording and quality management

- Phone, softphone and trunk recording:
  - Alcatel-Lucent OmniPCX RECORD Suite
  - Third-party recorders: DSPP

Emergency communication services

Building and campus emergency communications solution:

- 112 (EU), E911 (North America) services
  - Alcatel-Lucent Visual Notification Assistant (VNA)
  - Alcatel-Lucent Emergency Notification Server (ENS)
- Emergency Notification - Notify specific users about ongoing emergency calls

Hospitality communication services

- 8088 Smart DeskPhone
- ALE Enterprise, Essential, Premium DeskPhones, 8018 DeskPhone, or analog phones
- Guest features
- SIP phones
- Room service features
- Room directory features
- Billing and barring features
- Integration with Property Management Systems: DSPP

Architecture

System architecture

- 100% software architecture:
  - 100% IP, SIP communications
  - Communication Server
  - Software media services
- Hybrid architecture:
  - IP, SIP, digital, analog, DECT communications
  - Communication Server
  - Rack modules and Cabinets for media services and TDM connectivity

Capacity

- Single server or VMware delivery: 15,000 users (IP or SIP), 5000 TDM users, 9,000 Rainbow users
- 100 servers in a single network
- Fully networked servers, 100,000 IP/TDM users with single image
- 250 servers in a supra network
- More than 1 million users in a supra network
- BHCC per server: 300,000
- Software media services
  - IP, SIP, ABC network deployment
  - Up to 120 ports per virtual machine
  - G.711, G.729.AB, G.722
  - Transcoding
  - Ad hoc, meet-me and mastered audioconferencing
  - Dynamic voice guides

High availability

- Communication Server and database duplication
- Seamless communications failover
- Ethernet redundancy on INTIP-3, GD-4 and GA-4 boards
- Branch office full continuity with Passive Communication Server (PCS)

Communication Server platform

Industry servers

- Lenovo servers
- HP ProLiant DL servers

Virtual machines

- VMware vSphere
- Linux Kernel-based Virtual Machine (KVM)
- Microsoft Hyper-V
- Nutanix hypervisor - Acropolis OS

Hosted cloud platform

- In Alcatel-Lucent OpenTouch Enterprise Cloud (OTEC)

Optimized platform

- In Rack modules and Cabinets

Rack modules and Cabinets

OmniPCX Enterprise RM1 (19-in. rack)

- 3 modular slots (stackable up to 3 with RM3)
- Hot-swappable boards
- Height: 66 mm (2.60 in)
- Width: 442 mm (17.40 in)
- Depth: 400 mm (15.75 in)
- Weight: 10 kg (22 lb)

OmniPCX Enterprise RM3 (19-in. rack)

- 9 modular slots (stackable up to 3 with RM1)
- Hot-swappable boards
- Height: 154 mm (6.06 in)
- Width: 442 mm (17.40 in)
- Depth: 400 mm (15.75 in)
- Weight: 17 kg (38 lb)
- Power Supply: 150Watts

OmniPCX Enterprise M2 (cabinet)

- 1 ACT 28 or 2 ACT 14
- Hot-swappable boards
- Height: 740 mm (29.13 in)
- Width: 570 mm (22.44 in)
- Depth: 516 mm (20.31 in)
- Weight: 70 kg (154.32 lb)

OmniPCX Enterprise M3 (cabinet)

- 2 ACT 28 or 4 ACT 14
- Hot-swappable boards
- Height: 1500 mm (59.05 in)
- Width: 570 mm (22.4 in)
- Depth: 516 mm (20.31 in)
- Weight: 110 kg (242.5 lb)

OmniPCX Enterprise ACT 14-in data rack format (19-in. rack)

- 48 V power supply and battery backup
- Hot-swappable boards
- 1 ACT 14
- Height: 264.4 mm (10.41 in)
- Width: 486.3 mm (19.15 in)
- Depth: 383.4 mm (15.09 in)
- Weight: 30 kg (66.14 lb)

OmniPCX Enterprise ACT 28 in data rack format (19-in. rack)

- 48 V power supply and battery backup
- Hot-swappable boards
- 1 ACT 28
- Height: 530 mm (20.87 in)
- Width: 486.3 mm (19.15 in)
- Depth: 383.4 mm (15.09 in)
- Weight: 70 kg (154.3 lb)

Connectivity

- Hybrid SIP, IP, digital, analog switching
- IPv4 or IPv6 support

SIP

- SIP proxy/registrar/redirect server and SIP gateway
- Server redundancy (active/passive)
- Branch office survivability
- SIP Device Management for ALE devices and softphone

IPv6

- IPv6 and IPv4 dual stack
  - ¬ Communication server
  - ¬ RM1 and RM3
  - IPv6/IPv4 proxy
  - ¬ RM1 and RM3
- IPv6 or IPv4 stack
  - ¬ ALE DeskPhones (IP)

IETF standards

- SIP RFC: 1321, 2327, 2617, 2782, 2833, 2976, 3261, 2543, 3262, 3263, 3264, 3265, 3311, 3323, 3324, 3325, 3327, 3515, 3725 (partial), 3842, 3891, 3892, 3398, 3608, 3903, 3960 (partial), 3966 (partial), 4028, 4235, 4497, 4568, 4662, 4733, 4904, 5009, 5246, 5621, 5806, 6140, 7433, 7434
- RTP RFC: 1889, 1890, 2198, 3362, 3550, 3551, 3711

VoIP

- G.722 audio wideband
- G.711 A-law and µlaw, G.723.1A, G.729.AB audio
- Call admission control
- Automatic compression algorithm allocation
- Dynamic jitter buffer, echo cancellation, packet loss concealment (PLC), VAD: silence suppression and comfort noise generation
- DTMF Q23, robust DTMF relay, RFC 2833, in band DTMF
- Generic signal qualification and modem transport
- Anti-saturation mechanism; backward and forward automatic gain control
- Embedded signal quality diagnostic tool
- QoS: TOS or DiffServ tagging, 802.1 p/Q
- VoIP ticket for quality experience analysis

Fax

- G3, super G3 fall-back
- Automatic fax detection
- G.711 transparent and T.38 (Alcatel-Lucent protocol and SIP) and T38 with G711 fallback (SIP)

DECT

- DECT/GAP
  - ¬ Alcatel-Lucent 8212 DECT Handset
  - ¬ Third-party GAP handsets
- DECT/Alcatel-Lucent GAP (AGAP) for Premium Business Communications
  - ¬ Alcatel-Lucent 8232 8242, 8234, 8244, 8254, 8262, 8262EX DECT handsets
- Built-in controller
- Hybrid IBS/RBS and IP DECT networks
  - ¬ Alcatel-Lucent 8340 IP DECT Access Point
  - ¬ Alcatel-Lucent 8378 DECT IP-xBS base station
  - ¬ Alcatel-Lucent 8379 DECT IBS
  - ¬ Alcatel-Lucent 8318 SIP-DECT single Base station
- Advanced Radio Base Station (RBS)
  - ¬ Dedicated DECT8 board

VoWLAN

- Premium Business Communications
  - ¬ 8158s, 8168s WLAN Handsets in NOE mode
- Alcatel-Lucent OmniAccess® WLAN access points and WLAN controllers
  - ¬ Built-in QoS

Public networking protocols

- SIP, SIP/TLS, E164 support
  - ¬ Audio, video
- T0 ISDN
- T1-CCS ISDN (T2)
- E1CAS
- T1 CCS (PRI)
- T1 CAS
- DID/DDI or NDDI/non-DID analog networks

Private networking protocols

- Alcatel-Lucent ABC
  - ¬ User feature transparency
  - ¬ Network-wide management
  - ¬ Network-wide routing
  - ¬ Centralized applications
- IP
  - ¬ ABC based on enhanced QSIG (tunneling) and SIP for VoIP
  - ¬ SIP, H.323v2
  - ¬ ABC VPN for networking over ISDN/ PSTN network
  - ¬ ABC Direct IP Link
- TDM
  - ¬ ABC
  - ¬ QSIG BC, QSIG GF, DPNSS

Business process integration

Interfaces for Developer and Solutions Partner Program (DSPP)

- SIP
- XML web services
- CSTA, TSAPI Premium Server, TAPI Premium Server, RTI, WMI
- LDAP
- DR-Link (IP and TDM)
- Alcatel-Lucent Hospitality Link, InfoCenter
- OmniVista 8770 Ticket collector, OpenAPI and SNMP proxy
- QSIG, Paging Interface
- SNMP v3 for NMS integration
- OmniPCX Open Gateway (O2G): Call control, Management and Analytics

Security

Authentication

- Local or external RADIUS
- IEEE 802.1X TLS1.2
- Integrated audit tool to assess security management
- LDAPS authentication for OXE SIP Device Management

Traffic filtering
- Communication Server
  - ¬ Trusted hosts file
  - ¬ TCP wrapper function
- ALE DeskPhones
  - ¬ ARP spoofing protection
  - ¬ PC port switch VLAN filtering

Encryption for management
- SSHv2 for secure sessions (such as Telnet, FTP)
- TLS1.2 for secure HTTP session
- LDAPS for directory access

Native encryption
- Client/device confidentiality (signaling protocol and media)
- DTLS 1.2 with AES 256 and SRTP with AES 128
  - ¬ 100% software based
  - ¬ SHA2 certificate authentication
  - ¬ Enterprise, Essential, Premium DeskPhones (IP) and IPDSP
  - ¬ GD4/GD3/INTIP3/OMS and PCS
  - ¬ DTLS scalability with External Encryption Gateway
  - ¬ IP-XBS DECT encryption
  - ¬ Rainbow WebRTC Gateway encryption
- TLS 1.2 with AES 256 and SRTP with AES 128
  - ¬ SIP trunks

IP premium security encryption
- Client/device confidentiality (signaling protocol and media)
- IPSec and Secure RTP (AES 128 bits)
  - ¬ Premium DeskPhones (IP) and IP Touch
  - ¬ GD-3 and GA-3 boards
  - ¬ Alcatel-Lucent IP Premium Server Security Module
  - ¬ Alcatel-Lucent IP Premium Media Security Module
- Secure SIP/SRTP

Integrity
- Media gateway, Enterprise, Essential and Premium DeskPhones binary signatures

User policy enforcement
- Call monitoring and barring
- Internal toll fraud protection by class of services

Session Border Controller
- SIP perimeter defense:
  - ¬ Alcatel-Lucent OpenTouch Session Border Controller (OEM AudioCodes Mediant Virtual Edition)
  - ¬ Remote worker with 8008(G), 8018, 8028s, ALE-2, ALE SoftPhone

Operations

Element management
- Command Line Interface
- Web-based management
  - ¬ Configuration
  - ¬ Mass provisioning

Centralized operations
- Alcatel-Lucent OmniVista 8770 Network Management System
- Media and Management IP flows separation
- Cloud Connect Operations
  - ¬ Push licence files
  - ¬ Software upgrade
  - ¬ Inventory

European Directives and International Standards

EC Directives
- RED2014/53/EU
- 2011/65/EU: ROHS
- 2012/19/EU: WEEE
- 2014/30/EU: EMC
- 2009/125/EC: Ecodesign
- 2014/35/EU: LVD

Safety
- IEC 60950-1
- UL/CSA 60950-1
- IEC62368-1
- IEC62308-1

EMC
- IEC CISPR 32 Class B
- CENELEC EN 55032 Class B
- FCC Part 15B
- IEC CISPR24
- CENELEC EN 55024
- IEC EN 61000-3-2
- ICES-003

Miscellaneous environments
- ACT:
  - ¬ CENELEC EN 50121-4: Railway applications
- RM1, RM3:
  - ¬ DNV certificate: Maritime
  - ¬ IEC 60945: Maritime

Environmental conditions
- ETSI – ETS 300 019 Part 1-1: Storage
- ETSI – ETS 300 019 Part 1-2: Transportation
- ETSI – ETS 300 019 Part 1-3: In Use

Telecom
- ETSI EG 201 121
- ETSI ES 203 021
- ETSI ES 203 038
- ETSI TBR 010, 022, 003, 033, 004, 034, 008
- ITU-T H.323
- FCC Part 68
- Canada CS03

Alcatel·Lucent Enterprise

Alcatel·Lucent
Enterprise

M7 DeskPhone from Alcatel-Lucent Enterprise

The M7 DeskPhone from Alcatel-Lucent Enterprise offers a rich SIP communications experience with intuitive navigation and conversation comfort.

This elegant DeskPhone provides super wideband audio in hands-free mode with echo cancelling and double talk performance. The large 3.5" color screen, makes it quick and easy to connect.

The user experience is enhanced with a 4-way navigation key, 8 line keys, 4 soft keys and a user-friendly interface.

The M7 DeskPhone includes USB A/C ports making it more than a phone. It is possible to connect to a PC as an external loud speaker to take advantage of the super wide band speaker phone or plug external devices such as Expansion Module (EM20 or EM200), headset, conference module etc. The M7 DeskPhone supports a Wi-Fi dongle.

The M7 DeskPhone includes an adjustable foot stand and comes with customizable faceplates to promote brand awareness.

The standard SIP protocol provides the rich telephony features supported by the major open SIP servers in the market.

The M7 DeskPhone can operate in Power over Ethernet (PoE) mode (Class 2) and with a Wi-Fi dongle.

Features	Benefits
Bluetooth 4.1 connectivity	Connect a headset for wireless connectivity up to 10 meters From your desk. Supports a wireless handset option.
Super wideband audio quality	Super wideband audio for speaker phone and wideband audio for the handset
Large 3.5" color screen and 4-way navigation button	Easily navigate and connect with colleagues or customers
Elegant phone with adjustable foot stand	Perfect for small desks, hotel rooms and hospital bedsides
Customized faceplate	Display your organization's logo and create brand awareness
Rich telephony features with standard SIP protocol	Benefit from business features such as call management and conference, provided by your preferred cloud PBX provider
Effortless Deployment	Benefit from ALE Easy Deployment Server (EDS), and Easy Provisioning Sever (EPS); very easy to configure and deploy

Datasheet
Alcatel-Lucent Enterprise M7 DeskPhone

Technical specifications

Physical characteristics

- Height: 183mm (7.2 inches)
- Width: 207mm (8.2 inches)
- Depth: 35mm (1.4 inches)
- Weight: 810 (1.79 lbs) incl. handset and foot stand
- Color: Gray
- Adjustable foot stand: 40° and 55°
- Wall mountable

Display

- 3.5 inches color LCD
- 320x240

Keys

- 8 line keys with LED
- 4 menu keys
- Volume control keys (+ and -)
- Navigator: 4 way navigation + OK
- Hands-free, mute and message keys
- Call hold, call transfer and redial key
- Dial pad

Telephony features

- 8 SIP accounts
- Call forward, call waiting, call transfer, call hold/resume, redial
- Mute/unmute, voicemail, DND, auto answer
- Local 5-party conference
- Call log, local contacts (1000)

Audio characteristics

- G.722, OPUS, iLBC
- G711 (A-law and Mu-law), G.729AB
- VAD (Voice Activity Detection), Comfort Noise Generation (CNG)
- Acoustic echo cancellation
- DTMF: In-Band, RFC2833, SIP INFO
- Hearing Aid Compatible (HAC)

Power

- Power over Ethernet (IEEE 802.3af), Class 2
- External Power supply: 5V/2A (Optional accessory)

Connectivity

- RJ-45 LAN: 10/100/1000M Ethernet
- RJ-45 PC through 10/100/1000M Ethernet switch
- RJ-9 connector for corded handset
- USB Type A and USB Type C

Network and protocols

- SIP v2 (RFC3261)
- Static IP and DHCP
- IPv4/IPv6
- IEEE 802.1AB/LLDP-MED/QoS
- TR069

Configuration

- Web-based management
- ALE Easy Provisioning Server (EPS)
- ALE Easy Deployment Server (EDS)

Security

- Authentication: Basic or digest, 802.1x
- Denial of service (DoS) attack protection: Flooding
- ARP Spoofing protection
- Transport: TLS 1.2/1.0 and SRTP
- Shipped with (X509v3) certificate installed
  - Certificates for 802.1x EAP-TLS (either Alcatel-Lucent or customer certificates)
- Supporting SHA2 ALE Certificate, SCEP, OpenVPN

Languages

- Multi-language support (menu):
- Arabic, Chinese (simplified), Chinese (traditional), Czech, Danish, Dutch, English (American), English (British), Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Russian, Slovak, Slovenian, Spanish, Swedish, Turkish

Regulatory Standards

Safety

- EN 60950-1: 2006 +A11: 2009 +A1: 2010 +AC: 2011+A12: 2011 +A2:2013
- IEC 60950-1: 2005 +A1: 2009 +A2: 2013
- EN 62368-1: 2014 +A11: 2017
- CAN/CSA-C22.2 NO. 60950-1-07 +Am1: 2011 +Am2: 2014, ANSI/UL 60950-1-2014

EMC

- EN 55032, CISPR 32
- EN 55024, CISPR 24
- EN 61000-3-2, EN 61000-3-3
- FCC 47 CFR Part 15 B Subpart B
- ICES-003 Issue 6 Canada
- ETSI EN 301 489-1
- ETSI EN 301 489-17
- EN 55024
- CISPR 24
- CISPR 32
- EN 55032
- EN 61000-3-3 / IEC 61000-3-3

Eco design

- ErP 2009/125/EC, WEEE 2012/19/EU
- ROHS 2011/65/EU, CHINA ROHS 2: GBT 26572-2011
- REACH: European regulation: N° 1907/2006
- Proposition 65
- Packaging: EU Directive 94/62/EC

Hearing aid compatibility

- US: Section 68.316 (HAC) and 68.317 of FCC 47 C.F.R. Part 68
- Canada: CS-03 Part V, Issue 9 +Amendment 2
- Australia/NZ: AS/ACIF S040: 2001

Environmental Conditions

- Operating temperature: -5°C to +45°C
- Relative humidity: 5% to 95%
- Storage/transportation temperature: -25°C/+70°C

Accessories

- 3MK27006AA EM20 Expansion module
- 3MK27007AA EM200 Expansion module
- 3MK27008AA wall mounting kit
- 3MK08005US external power adapter (US)
- 3MK08005EU external power adapter (EU)
- 3MK08005RW external power adapter (AU/UK)

Packaging

- M7 DeskPhone
- Wired wideband handset
- Foot stand
- 1.5m Ethernet cable (cat5e)
- Safety sheet
- Quick user guide

89

Alcatel·Lucent Enterprise

Legal notice

Disclaimer

While efforts were made to verify the completeness and accuracy of the information contained in this documentation, this document is provided "as is". To get more accurate content concerning Cross Compatibilities, Product Limits, Software Policy and Feature Lists, please refer to the accurate documents published on the Business Partner Web Site.

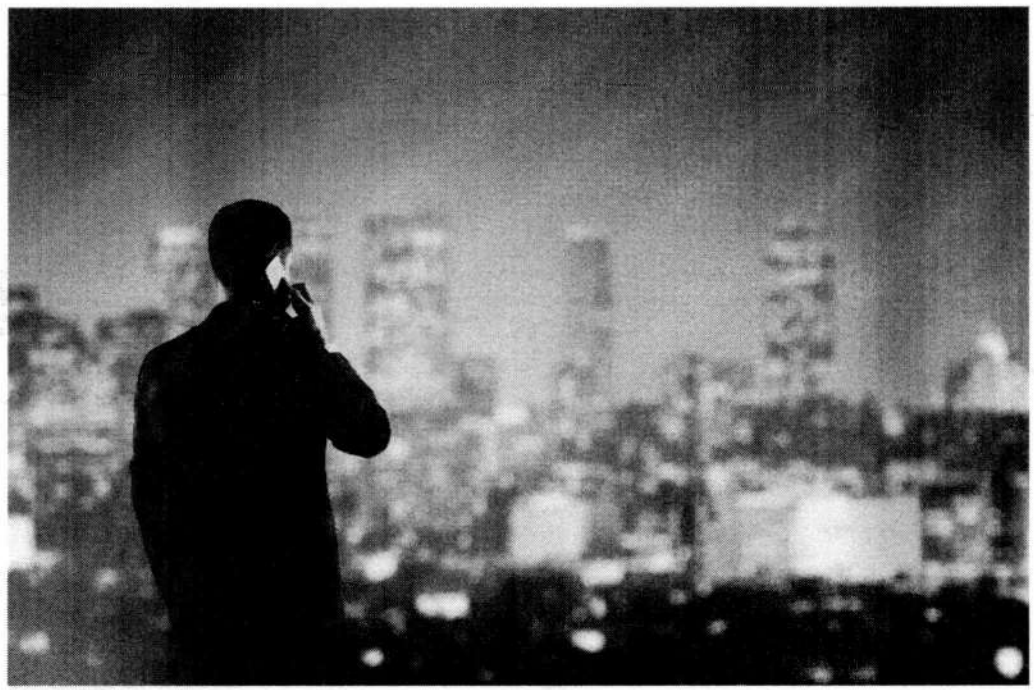
In the interest of continued product development, ALE International reserves the right to make improvements to this documentation and the products it describes at any time, without notice or obligation.

The CE mark indicates that this product conforms to the following Council Directives:

- 2014/53/EU for radio equipment
- 2014/35/EU and 2014/30/EU for non radio equipment (including wired Telecom Terminal Equipment)
- 2014/34/EU for ATEX equipment
- 2011/65/EU (RoHS)
- 2012/19/EU (WEEE)

CE

M Series Deployment Guide



June 2020

8AL90621ENAA 01

Alcatel·Lucent Enterprise

Table of contents

M Series Deployment Guide

92

Chapter 1

Introduction

This document describes the deployment of M Series DeskPhone sets with a third party SIP server.

The following sets are covered:

M3 DeskPhone 

M5 DeskPhone 

M7 DeskPhone 

The M Series DeskPhone Deployment Guide provides general guidance on setting up phone network, provisioning and managing phones.

This guide is not intended for end users, but for administrator with experience in networking who understand the basis of open SIP networks and VoIP endpoint environments.

As an administrator, this guide will enable you to do the following:

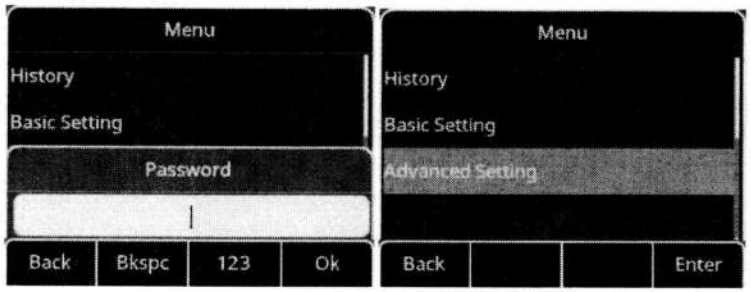
- Set up a VoIP network and provisioning server.
- Provision the phones with features and settings.
- Troubleshoot, upgrade and maintain phones.

The information detailed in this guide is applicable to the M Series DeskPhone sets running firmware version 2.10.13 or above (see: *Checking the software version of the phone set* on page 9)

Chapter 2

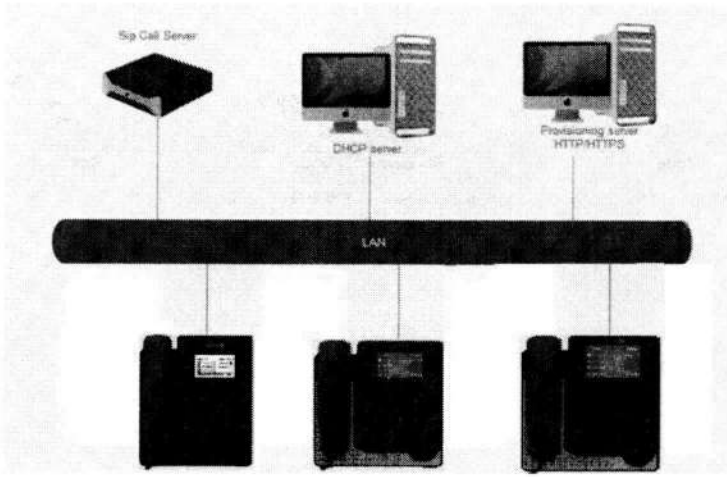
Glossary

DHCP	Dynamic Host Configuration Protocol
DM	Device Management = provisioning server
EDS	Easy Deployment Service
FQDN	Fully Qualified Domain Name
HTTP/HTTPS	Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MMI	Man Machine Interface
PoE	Power over Ethernet
RAM	Random Access Memory
SIP	Session Initiation Protocol
SSH	Secure Shell
URL	Uniform Resource Locator
USB	Universal Serial Bus
VCI	Vendor Class Identifier
WBM	Web Based Management
WAN	Wide Area Network



3.5 Network topology

There are many ways to set up a phone network using ALE SIP phones. The following figure shows the simplest example of a network setup.



3.6 Verifying startup

The phone begins the initialization process by following steps after connecting to the power and network:

1. The power LED indicator glows blue.
2. The message "Welcome" appears on the phone screen when the IP phone starts up.
3. Press the OK key on navigator keypad to check the status of the phone quickly. Phone information, such as the valid IP address, MAC address, firmware version will be displayed on the screen.

Chapter 3

Accessing phone set information

This chapter describes where M Series DeskPhone sets fit in your network, and provides basic initialization instructions of SIP phones.

3.1 Requirements

In order to perform as SIP endpoints in your network successfully, you need the following in deployments:

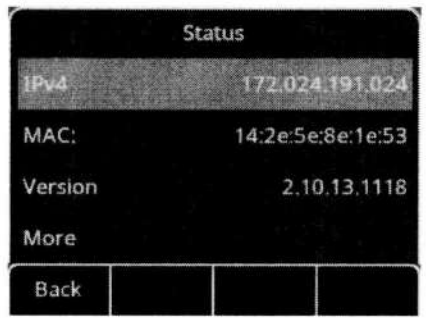
- M Series DeskPhone sets with compatible firmware (2.10 or above). To upgrade their firmware, see: Upgrading the firmware on page 34.
- A working IP network.
- An active SIP call server.
- A text editor, such as Notepad++, to create and edit configuration files.

3.2 Checking the device information

You can view the phone model information on the back of the phone. This label provides information on the phone model, SN and MAC address etc.

3.3 Checking the software version of the phone set

You can check the phone's software information by pressing the OK button in navigator keypad. This operation will allow the user to enter the status menu directly.



3.4 Checking the phone settings

After switching on the phone, press the "OK" button or "Menu" button and then select "Advanced settings" by pressing the navigator down key, then press the "OK" button to confirm, enter the password of "Admin" (password is "123456" by default).

Chapter 4 Phone set provisioning overview

4.1 Provisioning method priority

A priority order is defined between the different provisioning methods: settings you make using a higher priority provisioning method will override settings made using a lower priority method.

The priority order for setting provisioning is:

1. Settings received from the provisioning server (DM server)
2. Settings received from the DHCP server
3. Settings configured locally via MMI or WBM
4. Factory default settings

For the DM URL configuration, the priority is the following:

1. DM URL received from DHCP
2. DM URL configured via MMI or WBM
3. DM URL received from EDS

4.2 Configuring IP parameters and SIP account parameters via MMI

4.2.1 Configuring IP parameters via MMI

The setting menu of the MMI can be accessed when the phone is starting up:

1. At initialization (from **step 1: System initialization**), press the * and # keys to access the MMI.
2. Enter the admin password (the default admin password for the phone out of box is 123456).
3. Press the softkeys **IP param** > **IP config** > **IPv4 settings** to access the IP parameters setting page. This page allows you to select the initialization mode (The default DHCP mode is dynamic) and to configure network parameters if static mode is selected.
4. Press the softkey next to **IPv4 mode** to switch to **Static**.
5. Complete the set IP parameters:
   - **IP**: enter the set IP address
   - **S/net**: enter the IP subnet mask
   - **Router**: enter the default router IP address
6. Press the **OK** key to save modifications
7. Press release key to exit the settings menu.

The set automatically reboots to apply these settings changes.

4.2.2 Configuring SIP account parameters via MMI

The settings menu of the MMI can be accessed when the phone is starting up:

1. At initialization (from **step 1: System initialization**), press the * and # keys to access the MMI.
2. Enter the admin password (the default admin password for the phone out of box is 123456).
3. Press down key on navigator keypad until the last page and press **SIP servers** softkey.

Chapter 4 Phone set provisioning overview

This chapter gives general indication on the parameters that must be provisioned to start a set, the different ways to provision these parameters, and the priority rules between them.

Basically, parameters that must be provisioned are:

- IP parameters (IP address, netmask and router IP address)
- SIP account parameters (SIP server address, register name, username, password)
- DM URL, when SIP parameters are provisioned via SIP configuration files downloaded from a provisioning server

The different ways to provision these parameters are:

- IP parameters:
  - Statically via MMI: see Configuring IP parameters and SIP account parameters via MMI on page 12
  - Dynamically via DHCP
- SIP account parameters:
  - Manually:
    - Via MMI: see Configuring IP parameters and SIP account parameters via MMI on page 12
    - Via WBM: see Configuring IP parameters and SIP account parameters via WBM on page 13
  - Automatically via SIP configuration files downloaded from a provisioning server (DM server): see Building a SIP configuration file on page 28
- DM URL (required only in case of initialization with SIP configuration files):
  - Manually:
    - Via MMI: see Configuring the provisioning server URL via MMI on page 15
    - Via WBM: see Configuring the provisioning server URL via WBM on page 15
  - Automatically:
    - Via DHCP: see DHCP configuration for download path of SIP configuration files on page 22
    - Via EDS server: see Setting up auto-provisioning with EDS on page 32

The method you use depends on how many phones need to be deployed and what features and settings need to be configured. We recommend using manual provisioning as your primary provisioning method when just several phones are needed for testing.

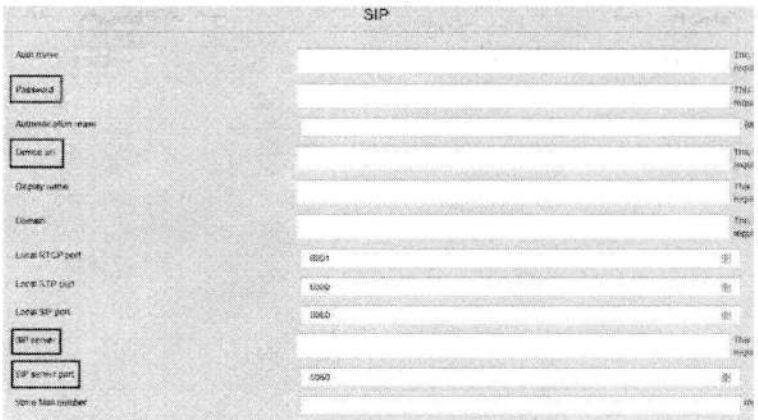
Commissioning phone sets on page 18 details four possible scenarios:

	IP Parameters	SIP parameters	DM URL
Scenario 1	MMI	MMI	N/A
Scenario 2	DHCP	WBM	N/A
Scenario 3	DHCP	DM server	DHCP
Scenario 4	DHCP	DM server	EDS

7. Enter the mandatory IP parameters in **Network** tab and press **Next**.

   On the new page you can configure the SIP account parameters as shown in the following figure.

   Note:
   The parameters highlighted in red in the figure below are mandatory for the phone set registration on the SIP server.



8. Press **Next**. You can skip the configuration on **LDAP** and **User** as they are not mandatory for the phone configuration at the first registration on the SIP server. Make sure all the mandatory fields have been filled in with correct value, then press **Confirm**. The phone reboots to apply these settings changes.

4. Select a SIP account and configure related SIP server connection parameters.
5. For details on SIP server parameters, see: SIP servers/groups/accounts on page 48.
6. Press the **OK** key to save modifications.
7. Press release key to exit the settings menu.

The set automatically reboots to take apply settings changes.

4.3 Configuring IP parameters and SIP account parameters via WBM

You can configure M Series DeskPhone sets via web user interface (WBM) when the phone has started up with proper IP parameters.

1. To find the IP address of the set, in the set user interface (MMI), select Settings > Network and read the IP address.
2. In a web browser, enter the URL: `https://[IP address]`, for example `https://192.168.0.10`
3. You are prompted to enter login/password:
   - login: enter **admin**
   - password: enter the password (default password is `123456`)
4. Click **Connect**
5. Change the password, and log in again with the new password

6. It is recommended to set up the phone via Wizard. Click the **Wizard start** to start the phone set configuration.

   The wizard includes five configuration steps as shown on the figure below. **Network** and **SIP** are mandatory for the first setup.

4.4 Configuring the provisioning server URL via MMI

The setting menu of the MMI can be accessed when the phone is starting up:

1. At initialization (from **step 1: System initialization**), press the * and # keys to access the MMI.
2. Enter the admin password (the default admin password for the phone out of box is `123456`).
3. Press down key on the navigator keypad to access the next page, and press the **DM** softkey.
4. Press the button next to **URL**, and enter the complete URL (for example: `https:// <provisioning server IP address>/download`).
   Note:
   *If the server requests HTTPS digest authentication, complete the **Username** and **Password** fields with the appropriate credentials).*
5. Press the **OK** key to save modification.
6. Press release key to exit the settings menu.

   The set automatically reboots to download the SIP configuration file from the provisioning server.

4.5 Configuring the provisioning server URL via WBM

You can configure M Series DeskPhone sets via web user interface (WBM) when the phone has started up with proper IP parameters.

1. To find the IP address of the set, in the set user interface (MMI), select Settings > Network and read the IP address.
2. In a web browser, enter the URL: `https://[IP address]`, for example `https:// 192.168.0.10`
3. You are prompted to enter login/password:
   - login: enter **admin**
   - password: enter the password (default password is `123456`)
4. Click Connect
5. If needed, change the password, and login again with the new password
6. Go to Settings > Network > DM
7. In the DM URL field, enter the complete URL (for example: `https://<provisioning server IP address>/download`).
   Note:
   *If the server requests HTTPS digest authentication, complete the **Username** and **Password** fields with the appropriate credentials).*
8. Press **Apply** to save modification.

   A reboot pop-up opens.
9. Press **Reboot now**.

   The set automatically reboots to download the SIP configuration file from the provisioning server.

4.6 Central provisioning with SIP configuration files

You can set up M Series DeskPhone sets using a SIP configuration file, downloaded by the set from a provisioning server using HTTP or HTTPS. The SIP configuration file contains necessary information to allow the M Series DeskPhone sets to register on the SIP server. The file name format is `config.{mac-address}.xml`.

For more information on the SIP configuration file content and structure, see:

- Description of the SIP settings in configuration file on page 47
- SIP configuration file templates on page 43

To configure a provisioning server in your network environment, see: Provisioning server setup overview on page 24.

The download path of SIP configuration file can be provisioned:

- Via DHCP: see Setting up a DHCP server on page 21
- Via EDS: see Setting up auto-provisioning with EDS on page 32
- Statically:
  - Via MMI: see Configuring the provisioning server URL via MMI on page 15
  - Via WBM: see Configuring the provisioning server URL via WBM on page 15

Chapter 5

Connecting the phone set to the customer network

Connecting the phone set to the customer network:

- If the phone set is powered by PoE:
  - **a.** Plug the RJ45 cable into the set LAN connector
  - **b.** Connect the RJ45 cable to the customer network via a PoE hub/switch (IEEE802.3af compliant)
- If the phone set is not powered by PoE, plug the AC/DC external adapter to the set power supply connector (DCSV) and connect the plug to the power supply

Once the phone set is connected and powered up, it automatically starts initializing.

The phone set begins the initialization process by following steps after connecting to the power and network:

1. The call and message LED indicators glow blue.
2. The message "Welcome" appears on the phone screen when the phone set starts up.
3. The main phone screen displays the following:
   - Firmware version on the top of the screen
   - Each initialization step, from step 1 to 5
4. Press right key on navigator keypad to enter the settings menu. The phone screen then displays the valid IP address, MAC address, phone configuration, firmware version, help for navigator key usage, and more.

Chapter 6

Commissioning phone sets

This chapter describes basic initialization instructions of M series DeskPhone sets.

Four scenarios are described:

- Scenario 1: IP static initialization on LAN, no SIP configuration file on page 18
- Scenario 2: IP dynamic configuration on LAN, no SIP configuration file on page 18
- Scenario 3: IP dynamic configuration on LAN with SIP configuration file (zero touch) on page 19
- Scenario 4: IP dynamic configuration on WAN with SIP configuration file (zero touch) on page 19

6.1 Scenario 1: IP static initialization on LAN, no SIP configuration file

Scenario 1 describes the commissioning of a set on the LAN with IP static initialization (no DHCP server) and without SIP configuration files (no provisioning server). In this scenario, all the configuration is performed via the set MMI.

Before beginning: you must know the following:

- IP parameters of the set (IP address, netmask, router IP address)
- SIP parameters: SIP call server information (IP addressing, domain, authentication)

Prerequisites:

- The M Series DeskPhone firmware is 2.10.13 or above.

  At initialization, the firmware version is displayed at the top of the screen: see: Checking the software version of the phone set on page 9

To commission the set:

1. Configure the phone set on the SIP call server as needed according to the SIP server documentation
2. Connect the set: see Connecting the phone set to the customer network on page 17
3. Access the phone set user interface (MMI) and configure the following:
   a. Change the initialization mode from **Dynamic** (default mode) to **Static**: see: Configuring IP parameters via MMI on page 12
   b. Configure the IP parameters of the phone set: see: Configuring IP parameters via MMI on page 12
   c. Configure SIP parameters (via a SIP account): see: Configuring SIP account parameters via MMI on page 12

6.2 Scenario 2: IP dynamic configuration on LAN, no SIP configuration file

Scenario 2 describes the commissioning of a set on the LAN with IP dynamic initialization (provision of standard IP parameters by DHCP server) and without SIP configuration files (no provisioning server). In this scenario, the sets gets its IP parameters from the DHCP server and SIP parameters are configured manually via WBM.

Before beginning: you must know the following:

- SIP parameters: SIP call server information (IP addressing, domain, authentication)

Prerequisites:

- The M series DeskPhone firmware is 2.10.13 or above.

set initialization from a provisioning server, whose URL is provided by the EDS server: this requires a specific configuration on the EDS server. In this scenario, the set starts without any manual operation via MMI or WBM (zero touch).

Before beginning: you must know the following:

- SIP parameters: SIP call server information (IP addressing, domain, authentication): this information is required to build the configuration file

Prerequisites:

- The M series DeskPhone firmware is 2.10.13 or above.

  At initialization, the firmware version displays on the top of the screen: see: Checking the software version of the phone set on page 9
- The phone set can reach the WAN
- The phone set must initialize in dynamic mode (default mode)
- A DHCP is operational on the LAN (no specific configuration required): see Setting up a DHCP server on page 21
- A provisioning server is operational on the WAN or Cloud: see Setting up a provisioning server on page 24
- A profile associated to the phone MAC address has been created on the EDS server to provision DM URL and certificate relative URL: see Setting up auto-provisioning with EDS on page 32

To commission the set:

1. Configure the phone set on the SIP call server as needed according to the SIP server documentation
2. Create and configure the SIP configuration file: see: Building a SIP configuration file on page 28
3. Deploy the SIP configuration file in the provisioning server relative directory
4. Connect the set: see Connecting the phone set to the customer network on page 17

   After startup, the set automatically begins initialization process. After the last initialization step, the set registers to the SIP server.

At initialization, the firmware version displays on the top of the screen: see: Checking the software version of the phone set on page 9

- A DHCP is operational on the LAN (no specific configuration required): see Setting up a DHCP server on page 21

To commission the set:

1. Configure the phone set on the SIP call server as needed according to the SIP server documentation
2. Connect the set: see Connecting the phone set to the customer network on page 17
3. Read the IP address on the phone set display
4. Access the phone set configuration via WBM: see Configuring IP parameters and SIP account parameters via WBM on page 13
5. Configure SIP parameters

6.3 Scenario 3: IP dynamic configuration on LAN with SIP configuration file (zero touch)

Scenario 3 describes the commissioning of a set on the LAN with IP dynamic initialization (provisioning of standard IP parameters by DHCP server) and with SIP configuration file which will be downloaded during set initialization from a provisioning server, whose URL is provided by the DHCP server: this requires a specific configuration on the DHCP server. In this scenario, the set starts without any manual operation via MMI or WBM (zero touch).

Before beginning: you must know the following:

- SIP parameters: SIP call server information (IP addressing, domain, authentication): this information is required to build the configuration file

Prerequisites:

- The M series DeskPhone firmware is 2.10.13 or above.

  At initialization, the firmware version displays on the top of the screen: see: Checking the software version of the phone set on page 9
- The phone set must initialize in dynamic mode (default mode)
- A DHCP is operational on the LAN and configured to provide the URL of the provisioning server (DM URL): see Setting up a DHCP server on page 21 and DHCP configuration for download path of SIP configuration files on page 22
- A provisioning server is operational on the LAN: see Setting up a provisioning server on page 24

To commission the set:

1. Configure the phone set on the SIP call server as needed according to the SIP server documentation
2. Create and configure the SIP configuration file: see: Building a SIP configuration file on page 28
3. Deploy the SIP configuration file in the provisioning server relative directory
4. Connect the set: see Connecting the phone set to the customer network on page 17

   After startup, the set automatically begins initialization process. After the last initialization step, the set registers to the SIP server.

6.4 Scenario 4: IP dynamic configuration on WAN with SIP configuration file (zero touch)

Scenario 4 describes the commissioning of a set on the WAN with IP dynamic initialization (provisioning of standard IP parameters by DHCP server) and with SIP configuration files which will be downloaded during

Parameter	DHCP option	Description
DM server	66	Identify one DM URL (link for SIP configuration file downloading), or IP address or FQDN with optional port: see *DHCP configuration for download path of SIP configuration files on page 22* *Note:* *DM stands for Device Management server and is another name for provisioning server.*
option 43 > sub-option 67	67	Sub-option of Option 43, to define the DM path: *DHCP configuration for download path of SIP configuration files on page 22*
Default user class	77	ictouch.class0

Table 7.1: Configuration for DHCP Option 12, Option 60 and Option 77

	M3	M5	M7
VCI (dhcp option 60) (not modifiable)	ictouch.0	ictouch.0	ictouch.0
Default user class (option 77) (not sent by default)	ictouch.class0	ictouch.class0	ictouch.class0
Default hostname (option 12) (sent by default)	M3-XXYYZZ*	M5-XXYYZZ	M7-XXYYZZ

Note: *XXYYZZ is last 3 bytes of MAC address

7.2 DHCP configuration for download path of SIP configuration files

The table below describes the different possibilities for the configuration on the DHCP server of the download path for SIP configuration files.

You can ignore this section if auto-provisioning with EDS is used (see Commissioning phone sets on page 18: scenario 4).

Table 7.2: Configuration of download path on DHCP

Option 66	Option 43 > sub option 67 (full path)	Option 43 > sub option 67 (relative path)	Download path
		√	Invalid combination
√			https://option 66/
√		√	https://option 66/sub-option 67/
	√		Sub-option 67
√	√		Sub-option 67

Chapter 7

Setting up a DHCP server

This chapter details the configuration of the DHCP server to be performed when M Series DeskPhone sets initialize in dynamic mode.

The DHCP can be used to provide standard IP parameters only (see Commissioning phone sets on page 18: scenarios 2, 4) or standard IP parameters and the DM URL (see Commissioning phone sets on page 18: scenario 3). When the DM URL is not provisioned by the DHCP server, no specific configuration is required on the DHCP server: only standard IP parameters are required.

You can skip this section if M Series DeskPhone sets initialize in static mode (see Commissioning phone sets on page 18: scenario 1).

If configured for dynamic IP address, the M Series DeskPhone set retrieves its network configuration parameters from the DHCP server during step 3 of its initialization.

DHCP option configuration for IPv4 on page 21 details the list of DHCP options supported by M Series DeskPhone sets.

DHCP configuration for download path of SIP configuration files on page 22 describes how to configure the download path of SIP configuration files on the DHCP server.

Note:

Configuring the download path is not required when auto-provisioning with EDS is used.

7.1 DHCP option configuration for IPv4

The following table lists common DHCP options for IPv4 supported by M Series DeskPhone sets.

Parameter	DHCP option	Description
Subnet Mask	1	Specify the client's subnet mask
Router	3	Specify a list of IP addresses for routers on the client's subnet
Domain Name Server	6	Specify a list of domain name servers available to the client
Host Name	12	Specify the name of the client. (sent by default)
Domain Server	15	Specify the domain name that client should use when resolving hostnames via DNS
Network Time Protocol Servers	42	Specify a list of NTP servers available to the client by IP address
Vendor-Specific Information	43	Identify the vendor-specific information
Vendor Class Identifier	60	Identify the vendor type (ictouch.0)

Table 7.3: Configuration example for download path

Option 66	Option 43 > sub option 67 (full path)	Option 43 > sub option 67 (relative path)	Download path
192.168.2.2/ale/config			https://192.168.2.2/ale/config
192.168.2.2		ale/config	https://192.168.2.2/ale/config
	192.168.2.2/ale/config		https://192.168.2.2/ale/config
	http://192.168.2.2/ale/config		http://192.168.2.2/ale/config

Chapter 8

Setting up a provisioning server

8.1 Provisioning server setup overview

A provisioning server is necessary when SIP configuration files are used (see Commissioning phone sets on page 18: scenarios 3, 4).

You can skip this section if M Series DeskPhone sets initialize without SIP configuration files (see Commissioning phone sets on page 18: scenarios 1, 2).

M Series DeskPhone sets support the following transport protocols for provisioning:

The HTTP/HTTPS provisioning server can be set up on the local LAN. Use the following procedure as a recommendation if this is your first provisioning server setup.

To set up the provisioning environment:

1. Install an HTTP/HTTPS server application or locate a suitable existing server.
2. Create an account and home directory.
3. Set security permissions for the account.

Once the setup has been completed, create the SIP configuration files required for set commissioning (see: Building a SIP configuration file on page 28), and copy them in the HTTP/HTTPS provisioning server relative directory.

If the M Series DeskPhone set has retrieved a DM URL from the DHCP server, it downloads the configuration file from the provisioning server during step 4 of its initialization.

Note:

The DM URL which is configured in the DHCP server corresponds to the path of the SIP configuration files stored on the provisioning server.

8.2 Example with the Apache HTTP server setup

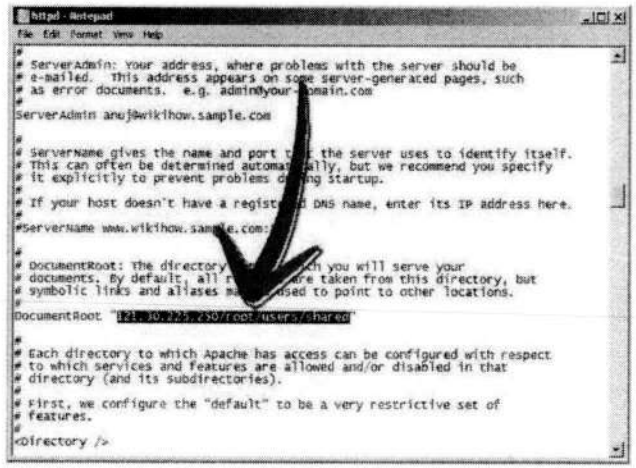
Configure a Windows server system (or virtual system) to set up an Apache web server with following standard steps. When the Apache web server has been successfully installed, create a directory on this server to store the SIP configuration files or firmware binary files, and get the download URL for set commissioning.

To set up an Apache HTTP server

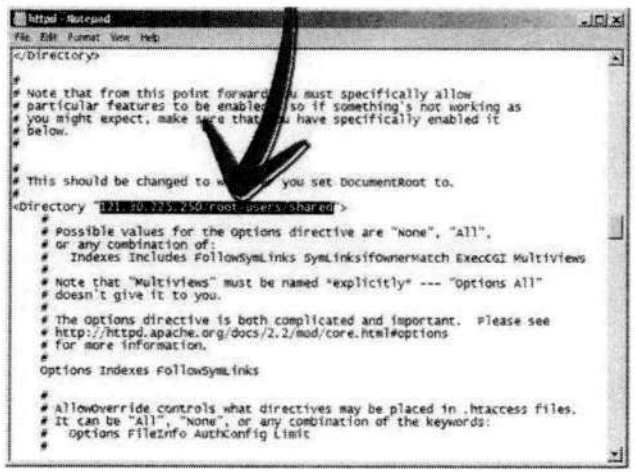
1. Go to *www.apache.org* and download the last version of Apache web server
2. Install the Apache web server

   When installing Apache, you are asked to enter your domain name, network name, and e-mail address. You can add any value in these fields. The format must be:

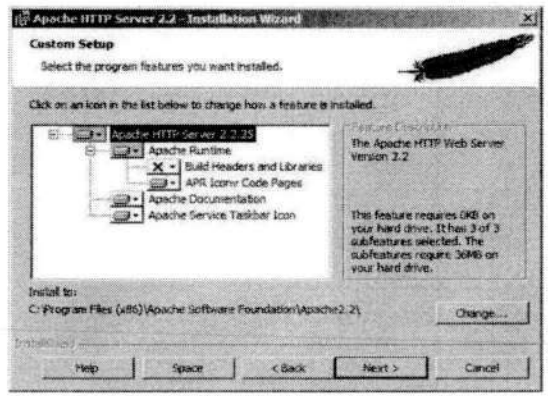
   - Domain name: `example.com`
   - Network name: `www.example.com`
   - E-mail address: `user@example.com`
3. Click **Next**
4. Select the Apache HTTP server from the radio button list



8. Repeat this operation for <Directory "drive:/location">

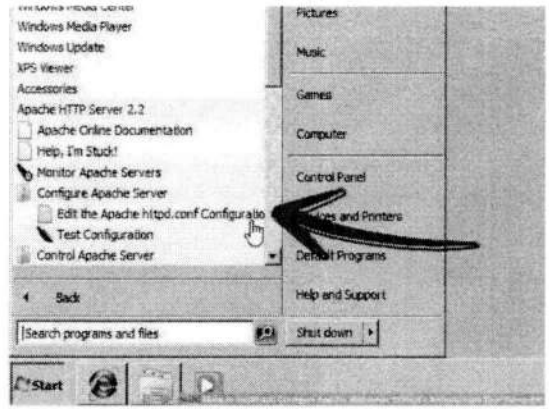


9. To verify your configuration, go to Apache in your taskbar and stop the service



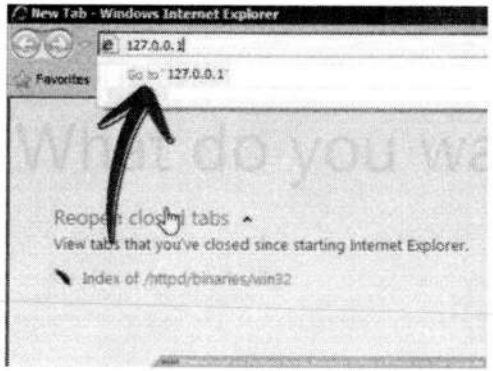
An error message is displayed such as: "Apache could not be configured. Edit your Apache.conf file"

5. Go to: **Start** > **Programs** > **Apache HTTP Server <version number>** > **Configure Apache Server** > **Edit the Apache httpd.conf Configuration File**



6. Go to the **DocumentRoot** line

7. Change the document root to point to the location of your website folder, using the character "/" instead of "\"



Note that, for most of users, to establish one Apache server is too complex, we strongly recommend you using some software tool to simulator Apache server, like MobaXterm, HFS etc.. These tools can also provide HTTP service but they are very easy to download and configure. See: Example with MobaXterm tool for provisioning on page 28.

8.3 Building a SIP configuration file

Before beginning, you must have the following:

- The MAC address of the phone set required for the name of the SIP configuration file (`config.{mac address of the phone set).xml`, for example `config.00809fe7021e.xml`): see Checking the device information on page 9
- A text editor, such as Notepad++, to create and edit configuration file

Build the SIP configuration file required for set commissioning:

1. Install an HTTP server application or locate a suitable existing server.

   For details on the file structure, name and minimum settings, see: SIP configuration file templates on page 43.

2. Complete the SIP configuration file according to your needs.

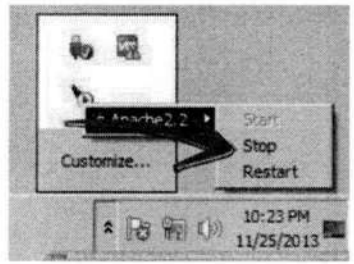
   For details on the available settings, see: Description of the SIP settings in configuration file on page 47.

Once created, copy the SIP configuration file in the HTTP/HTTPS provisioning server relative directory.

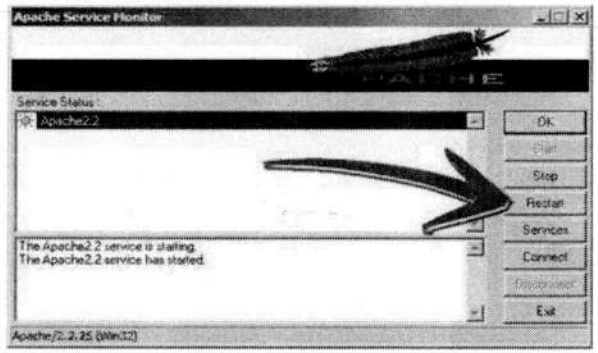
8.4 Example with MobaXterm tool for provisioning

Step1: Preparing the config file: `config.{mac-address}.xml`

In the config file the following contents should be included at the least:

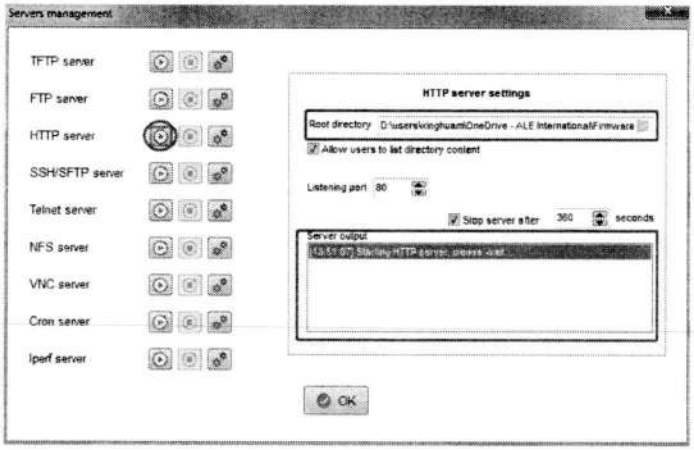


10. Restart the service



If the service does not start, modify the Apache httpd.conf configuration file properly

11. Once the service is restarted, open a web browser and enter `localhost` or `127.0.0.1` in the address bar

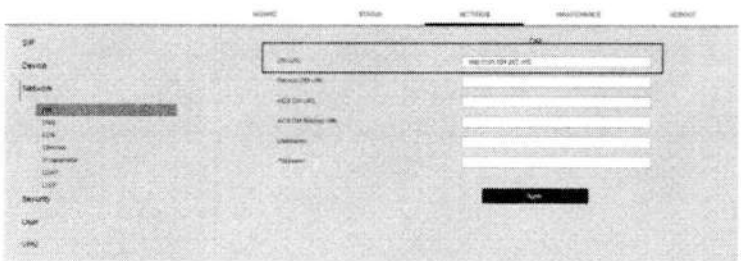


Note: you will see the "Starting HTTP server, please wait..." log in "Server output" box.

Step 5: Check the IP address of your PC, "135.251.222.150" for example.

Step 6: Log in the phone via web with default password "123456" and then change the password to complex one like "Ale123!@".

Then go to Settings---> Network---> DM---> DM URL, and fill in the path. The path is equal to the value of blue box field shown in the image1.



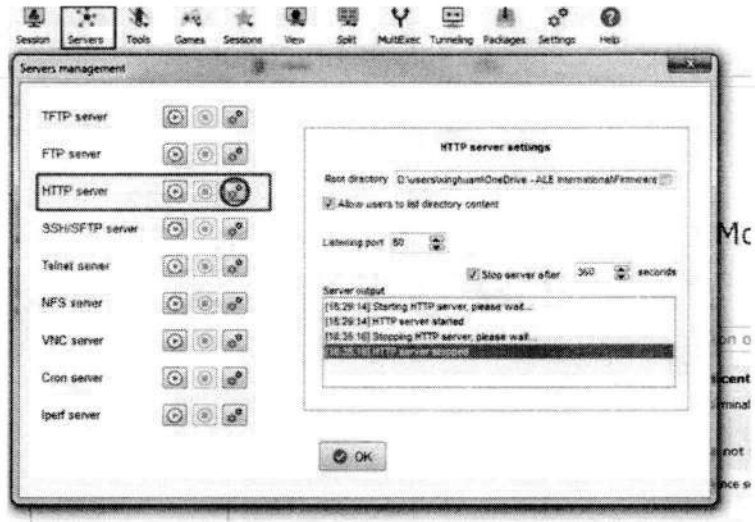
Step 7: Press "Apply". Then press "Reboot now" in the warning page.


```
<?xml version="1.0" encoding="UTF-8" ?>
<settings>
<setting id="SIPServerLAddress" value="TestSipDomain.sipserver.com" override="true"/>
<setting id="SIPGroupIDeviceUri" value="Testnumber" override="true"/>
<setting id="SIPGroupIAuthenticationPassword" value="TestSipPassword" override="true"/>
<setting id="DmAdminPasswd" value="000000" override="true"/>
</settings>
```

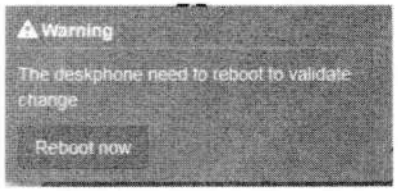
Note: For details on the file structure, see: SIP configuration file templates on page 43.

Step2: Install the MobaXterm tool on your PC.

Step3: Open the tool and go to "Servers → HTTP server → "settings" (red circle)



Step 4: Copy the path with the config file saved on your PC in "Root directory" and then press  to run the HTTP server on your PC.



Step 8: The phone will restart and then download the config file.

When the phone is starting up its admin password will be "000000" which is defined in config file with `sentence "<setting id="DmAdminPasswd" value="000000" override="true"/>"`

You can define the password by modifying the value.

Chapter 9 Setting up auto-provisioning with EDS

M Series DeskPhone sets support zero touch deployment by the Easy Deployment Service (EDS). You can contact the ALE EDS administrator *account.eds@al-enterprise.com* to create an account.

ALE EDS is a server side service that helps M Series DeskPhone sets to connect to the provisioning server on first startup. The service is deployed on the Internet Cloud.

The EDS server enables the provisioning of sets with the DM URL and certificates, allowing them to initialize from the WAN (see Commissioning phone sets on page 18: scenario 4), without requiring a specific configuration of the DHCP server.

When the set starts in dynamic mode and no provisioning server URL (DM URL) is configured via MMI or received from DHCP, it tries to connect to the ALE EDS server, whose address is hard-coded in its software. The server verifies the set's MAC address, and searches a profile for the set in the database.

The provisioning server URL and certificate relative URL are provided in the profile. The set downloads certificate, connects to the provisioning server via this URL, and downloads its SIP configuration file.

Note:

Auto-provisioning with EDS does not apply to phone sets initializing in static mode.

Chapter 10

Upgrading the firmware

This chapter details the firmware upgrade of M Series DeskPhone sets.

Before upgrading firmware, you need to know the following:

- Do not close and refresh the browser when the IP phone is upgrading firmware via web user interface.
- Do not unplug the network cables and power cables when the IP phone is upgrading firmware.

10.1 Upgrading by WBM

1. Put the new firmware version on your local PC
2. Connect to the set WBM (as explained in Configuring IP parameters and SIP account parameters via WBM on page 13) and go to: **Maintenance** > **Binary Update**
3. Click **Add binary files**
4. Select the binary file:
   - bin9000N
   - sip9000N

   Note:

   The header file is not necessary when upgrading by WBM.

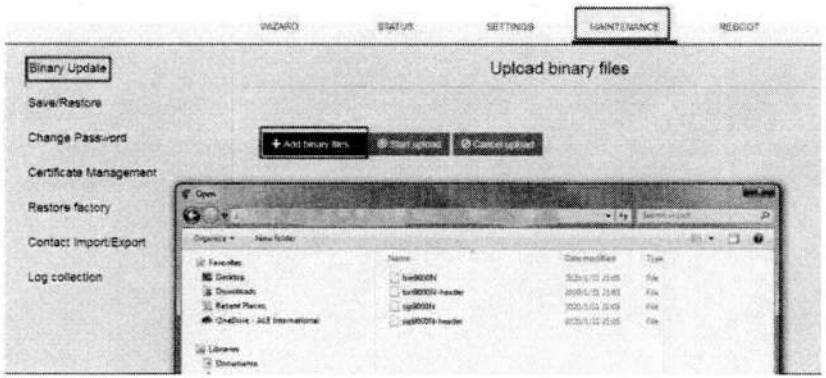


Figure 10.1: Binary file selection example

5. Click **Start upload**

Once downloaded, the phone installs the new binary and reboots. The whole process takes about 10 minutes in background (except reboot). A message is displayed when the binary upgrade is successfully completed.

On the phone set, you can check the version from the settings menu (see: Checking the software version

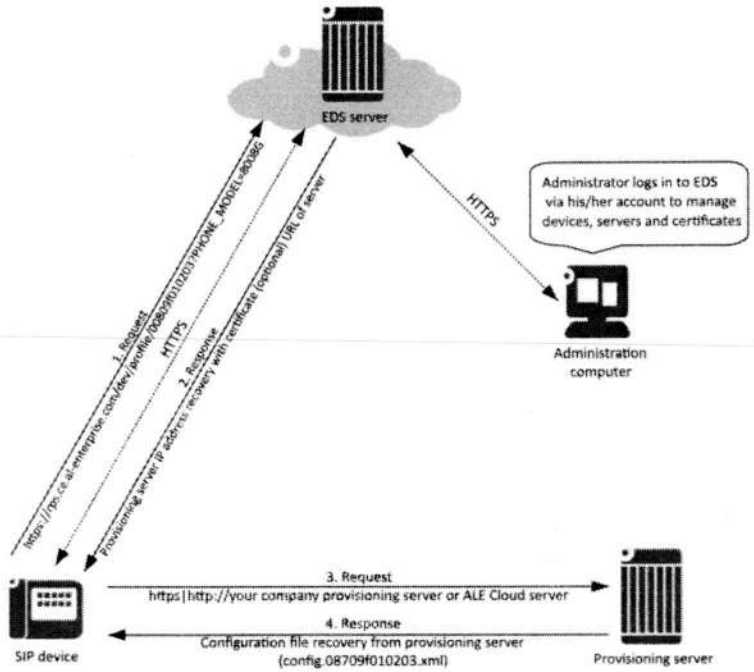


Figure 9.1: Auto provisioning process with EDS

of the phone set on page 9).

10.2 Upgrading by configuration file

You can upgrade the M Series DeskPhone sets using the SIP provisioning server and SIP configuration with relevant parameters.

M Series DeskPhone sets can be upgraded by downloading firmware binary files from a provisioning server whose URL must be defined in the SIP configuration file (i.e. `config.{mac-adress}.xml`, for example `config. 00809fe7021e.xml`).

Settings:

```
<setting id="DmEnetcfgUpgradeFile" value="upgrade URL" override="true"/>
```

Description:

Set up the upgrading URL. Enter the firmware binary file in the directory of provisioning server, for example the URL could be `http://192.168.2.2/ale/firmware`. Then this settings should be:

```
<setting id="DmEnetcfgUpgradeFile" value="http://192.168.2.2/ale/firmware" override="true"/>
```

You can trigger an immediate upgrade by resetting manually the M Series DeskPhone set, or enable automatic update by adding settings described below in the SIP configuration file.

Automatic update operates in the following way:

- The phone polls for new binary once a day at the time defined by `DmAdmcfgUpdateTimeStart`
- To prevent all sets from updating at the same time, `DmAdmcfgUpdateTimeDelta` can be configured so that each set will update at a random time between `DmAdmcfgUpdateTimeStart` and `DmAdmcfgUpdateTimeStart` + `DmAdmcfgUpdateTimeDelta`. In this way, upgrade parameters are the same for all sets, but each sets will update at a different time.
- If the directory contains a different version (older or newer), the set updates with this version
- If no binary file is available on the server, or the version is the same, nothing happens

The following settings are for the SIP configuration file template used for the phone upgrade at phone startup (no daily polling for automatic update).

```
<?xml version="1.0" encoding="UTF-8" ?>
<settings>
<setting id="DmAdmcfgUpdateTimeEnable" value="true" override="true"/>
<setting id="SIPServer1Address" value="TestSipDomain.sipserver.com" override="true"/>
<setting id="SIPGroup1DeviceUri" value="Testnumber" override="true"/>
<setting id="DmEnetcfgUpgradeFile" value="http://192.168.2.2/ale/firmware" override="true"/>
</settings>
```

1. Prepare the SIP configuration file and put it on the SIP provisioning server
2. Enter the firmware binary on the SIP provisioning server
3. Start the phone

   The phone downloads the SIP configuration file and reboots to enter the upgrading process. The phone reboots automatically after completing the entire upgrading process.
4. When the phone restarts, check that it has been upgraded to the desired version (see: Checking the software version of the phone set on page 9)

Chapter 11 Troubleshooting

11.1 Activating SSH

Some procedures in the following sections require to connect to the phone set via SSH. By default, SSH is deactivated and must be enabled via WBM, or `DmSecucfgSsh` parameter in the SIP configuration file of the phone set.

Once SSH is enabled, you can connect as admin by SSH. SSH login is "admin" and password is the same as admin password for MMI and WBM.

11.1.1 Activating SSH via WBM

1. Connect to the set WBM and go to: **Settings** > **Security** > **SSH**
2. Enable **SSH activation** and click **Apply**

11.1.2 Activating SSH via SIP configuration file

1. Download the target SIP configuration file from the HTTP/HTTPS provisioning server relative directory
2. Edit the SIP configuration file via a text editor
3. Insert or modify the `DmSecucfgSsh` command line as follows:

   ```
   <setting id="DmSecucfgSsh" value="true" override="true"/>
   ```
4. Upload the target SIP configuration file to the HTTP/HTTPS provisioning server relative directory
5. Reboot the phone set

11.2 Terminal information check (mandatory)

It is mandatory to provide the terminal information for each issue.

```
:id full      // To get the hardware & software information
:config       // To get the phone configuration
```

11.3 Collecting debug information (getlogs command)

The `getlogs` command allows you to collect and store debug information (logs) in an archive file. By default, this archive file is stored in the `/tmp` folder, with its filename provided on the console.

```
getlogs [usb[fallback] | flash [leds|popup|onreboot]] [list|clean|help]
```

Where:

- `usb[fallback]`: default storage on USB disk with or without fallback to flash storage
- `flash`: default storage on flash storage
- `leds|popup`: to list LEDs or show a pop-up window when obtaining logs

- onreboot: to delay the request to obtain logs at the next reboot
- list|clean: to list or clean logs on flash storage

Examples:

- Get logs immediately. Logs are stored in the /tmp folder and do not survive a reset.

```
getlogs
############### ... building archive file ...
############### /tmp/00809FF7794C-logs-output.log
############### /tmp/00809FF7794C-logs.tar.gz
############### ... please wait for the prompt ...
############### WARNING !!! Since the /tmp folder is not flashed, the file will not survive a
reset ###############
############### /tmp/00809FF7794C-logs.tar.gz can now be downloaded
```

- Get logs immediately to USB key, provided that a USB disk is present.

```
getlogs usb
```

- Get logs immediately to flash (/data/getlogs/) that can survive a reset.

```
getlogs flash
```

- Get logs on to flash reboot. Logs are stored in /data/getlogs.

```
getlogs flash onreboot
```

- Get logs on to a USB disk on reboot. Logs are stored on the connected USB disk

```
getlogs usb onreboot
```

- Get logs on to a USB disk on reboot. Logs are stored on the connected USB disk or (if not present) on flash.

```
getlogs usb fallback onreboot
```

11.4 Collecting system logs

The following commands allow you to collect the system logs of the phones.

```
$ cd /log/
$ ls -l
$ tar cvzf /tmp/syslog.tgz *.*
```

Several types of system logs are stored in the folder /log/:

- Defence.log
- Reset.log
- log.rcS
- pltf.log
- upgrade.log

After executing above commands, you may download the syslog.tgz file under /tmp/ and send it to ALE International for further analysis.

11.5 Collecting SIP telephony trace

If the issue is related to SIP telephony, below commands are necessary for debugging.

The different trace levels are:

- debug
- emerg
- err (default level)
- info
- notice
- warning

The type of logs collected depends on the level: for example, the err level allows you to collect only the error logs, whereas the debug level allows you to collect all logs.

Note:

The debug level takes more CPU load and memory usage which has an impact on the phone performance. That's why the level should be set to debug only for debugging purposes, and should be set back to err when there are no more errors or after all the necessary log information has been captured.

To get the SIP general information and status:

```
$ dumpsip                  //To show the basic SIP settings
$ dumpTelephony           //To show the SIP telephony status
```

To check and set the trace level and collect the trace of telephony:

```
$ level                    //To show the trace level
   ACTIVITY          LEVEL      SUPPORT        DESTINATION
ApplicationManager   err        file       /var/log/ApplicationManager.log
ictaudio             err        file       /var/log/ictaudio.log
ICTCliGateLite       err        file       /var/log/ICTCliGateLite.log
ictsipua             err        file       /var/log/ictsipua.log
LoggerModule         err        file       /var/log/LoggerModule.log
no facility          err        file       /var/log/no facility.log
Platform             err        file       /var/log/Platform.log
SettingsManager      err        file       /var/log/SettingsManager.log
sipmmi               err        file       /var/log/sipmmi.log
Telephony            err        file       /var/log/Telephony.log   //location of Telephony log
$ level Telephony debug     //To set the Telephony log to debug level
```

11.6 Collecting core dump files after crash issue

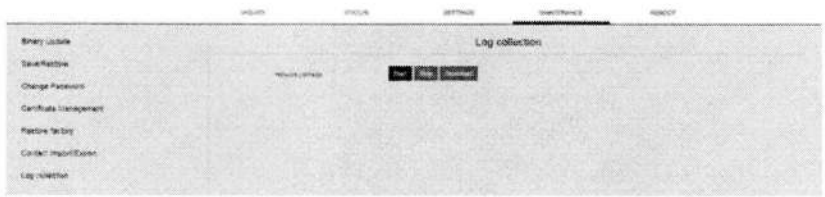
If a crash issue is detected, collect the related core dump files as below:

```
$ cd /data/core/
$ ls -l
drwxrwxr-x     2 admin    admin          400 Jul 31  15:20 .
drwxr-xr-x     6 root     root           424 Aug  3   2017 ..
-rw-r--r--     1 root     root      332221 Jul 31 15:20 core.ictbtmgr.gz     //core dump file
-rw-r--r--     1 root     root      177122 Jul  4   2006 core.ictsipua.gz     //core dump file
-rw-r--r--     1 root     root     1335296 Jun 23 10:22 core.sipapp_mgr.gz  //core dump file
```

11.7 Collecting audio trace

To check and set the trace level and collect the trace of audio:

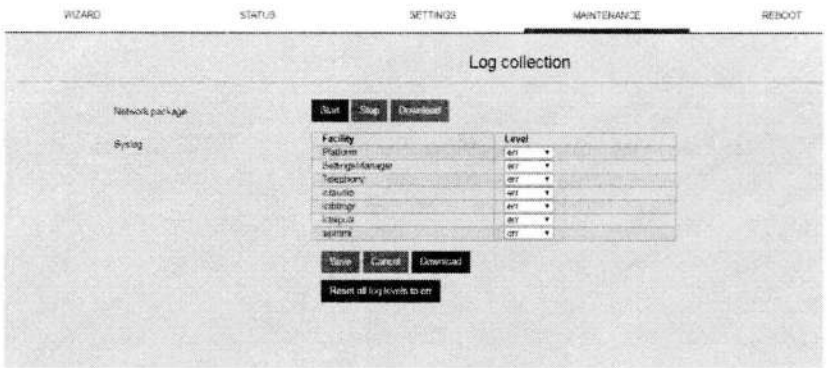
```
$ level                    //To show the trace level
```



2. Press the **Start** button to start the network capturing
3. Once the capturing trace is done, press the **Download** button to save the trace on your PC

To set the log level and download logs via WBM:

1. Log in to WBM and go to: **Maintenance** > **Log collection**



2. Select the trace/log levels for the different facilities and click **Save**
   Note:
   The `debug` level takes more CPU load and memory usage which has an impact on the phone performance. That's why the level should be set to `debug` only for debugging purposes, and should be set back to `err` when there are no more errors or after all the necessary log information has been captured.
3. Click **Download** to save traces/logs on your PC

11.10.2 Accessing logs from a syslog server

To retrieve SIP phone log files using a syslog server:

1. Connect to the device under test via SSH and login as admin
2. Use the following command to change all logs with debug level

```
$ level all debug
```



```
  ACTIVITY              LEVEL     SUPPORT         DESTINATION
ApplicationManager      err       file       /var/log/ApplicationManager.log
ictaudio                err       file        /var/log/ictaudio.log    //location of ictaudio
log
ICTCliGateLite          err       file       /var/log/ICTCliGateLite.log
ictsipua                err       file       /var/log/ictsipua.log
LoggerModule            err       file       /var/log/LoggerModule.log
no facility             err       file       /var/log/no facility.log
Platform                err       file       /var/log/Platform.log
SettingsManager         err       file       /var/log/SettingsManager.log
sipmmi                  err       file       /var/log/sipmmi.log
Telephony               err       file       /var/log/Telephony.log
$ level ictaudio debug  //To set the ictaudio log to debug level
```

```
$ voicemode             //To check current voice mode.
$ rtp 0                 //To check current rtp status
$ rtp 1                 //To check current rtp status
```

11.8 Collecting dbus messages

The dbus messages deal with communications between different applications (processes) in the phone.

Export the dbus messages into a file as below, and download this file for ALE International analysis.

```
$ cd /tmp/
$ dbus-monitor > /tmp/dbuslog    //To save the dbus messages into a file.
```

11.9 Collecting trace after MMI issue

For MMI issues, it is better to record a video for better understanding.

To collect the trace for MMI:

```
$ level                 //To show the trace level
  ACTIVITY              LEVEL     SUPPORT         DESTINATION
ApplicationManager      err       file       /var/log/ApplicationManager.log
ictaudio                err       file       /var/log/ictaudio.log
ICTCliGateLite          err       file       /var/log/ICTCliGateLite.log
ictsipua                err       file       /var/log/ictsipua.log
LoggerModule            err       file       /var/log/LoggerModule.log
no facility             err       file       /var/log/no facility.log
Platform                err       file       /var/log/Platform.log
SettingsManager         err       file       /var/log/SettingsManager.log
sipmmi                  err       file       /var/log/sipmmi.log    //location of sipmmi log
Telephony               err       file       /var/log/Telephony.log
$ level sipmmi debug    //To set the sipmmi log to debug level
```

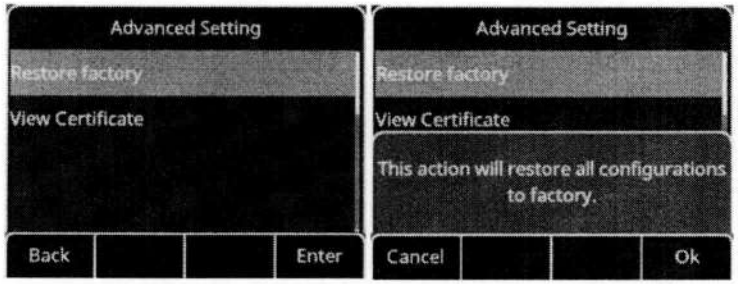
11.10 Accessing logs

You can retrieve the SIP phone log files from WBM or using a syslog server.

11.10.1 Accessing logs from the set Web Management

To capture network traces via WBM:

1. Log in to WBM and go to: **Maintenance** > **Log collection**

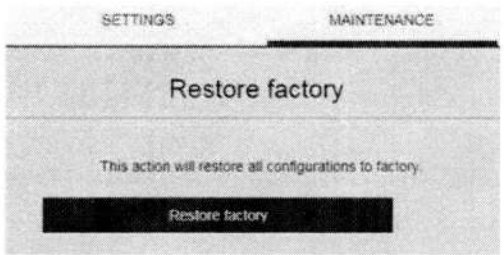


4. Select **OK** to confirm

11.11.2 Factory reset from WBM

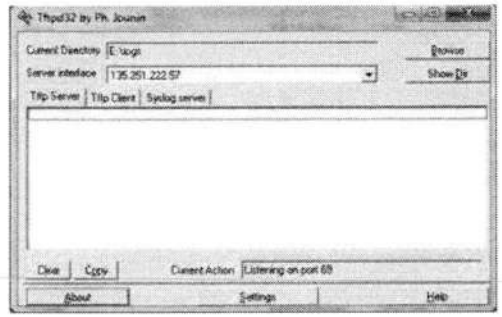
To perform a factory reset from the phone web based interface:

1. Log in to WBM and go to: **Maintenance** > **Restore factory**
2. Click **Restore factory**

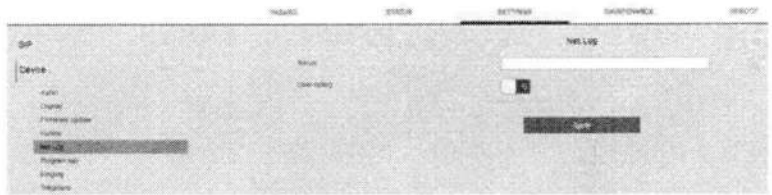


The phone restarts with all parameters restored to their factory values: this includes IP parameters and the set restarts in dynamic mode.

3. Install and start up a syslog server locally. For example:



4. Log in to WBM and go to: **Settings** > **Device** > **Net Log**
5. Fill in the related contents and enable **User netlog**



You will obtain the log files via syslog server.

11.11 Factory Reset

11.11.1 Factory reset from MMI

To perform a factory reset from the MMI:

1. On the phone set, press the navigator right key to display the menu list
2. Select **Advance Setting** and enter the password (default password:123456)
3. Press the navigator down key to display the last page and select **Restore factory**

```
    <setting id="ForwardBusyState" value="false" override="true"/>
    <setting id="ForwardBusyDest" value="" override="true"/>
<setting id="ForwardNoReplyState" value="false" override="true"/>
    <setting id="ForwardNoReplyDest" value="" override="true"/>
    <setting id="ForwardNoReplyOnCode" value="" override="true"/>
    <setting id="ForwardNoReplyOffCode" value="" override="true"/>

    <!--DND setting -->
 <setting id="DndModeAccount" value="0" override="true"/>
 <setting id="TelephonyDndMethod1" value="0" override="true"/>

    <!--phone mode -->
    <setting id="TelephonyDndState" value="false" override="true"/>
    <setting id="TelephonyDndOnCode" value="" override="true"/>
    <setting id="TelephonyDndOffCode" value="" override="true"/>

    <!--Account1 setting -->
    <!--Account1 SIP settings-->
    <setting id="SIPGroup1AuthenticationName" value="Registername" override="true"/>
    <setting id="SIPGroup1AuthenticationPassword" value="password" override="true"/>
    <setting id="SIPGroup1DeviceUri" value="Username" override="true"/>

<setting id="SIPGroup1DisplayName" value="display name" override="true"/>
    <setting id="SIPGroup1DtmfMode" value="2" override="true"/>
    <setting id="SIPGroup1SessionTimer" value="0" override="true"/>
    <setting id="SIPGroup1SessionTimerRefresher" value="0" override="true"/>
    <setting id="SIPGroup1SIPsURIUsage" value="false" override="true"/>
    <setting id="SIPGroup1SrtpWorkingMode" value="0" override="true"/>
    <setting id="SIPGroup1TLSAnticipation" value="false" override="true"/>
    <setting id="SIPGroup1TransportMode" value="0" override="true"/>
    <setting id="SIPGroup1ServerType" value="0" override="true"/>
    <setting id="SIPServer1Address" value="sip server address" override="true"/>
    <setting id="SIPServer1GenericPollingTimer" value="40" override="true"/>
    <setting id="SIPServer1GroupNumber" value="1" override="true"/>
    <setting id="SIPServer1KeepAliveEnable" value="true" override="true"/>
    <setting id="SIPServer1Port" value="5060" override="true"/>
    <setting id="SIPServer1RegisterExpire" value="3600" override="true"/>
    <setting id="SIPServer1FailoverAddress" value="" override="true"/>
    <setting id="SIPServer1FailoverPort" value="5060" override="true"/>
    <setting id="SIPServer1FailoverRegisterExpire" value="3600" override="true"/>
    <setting id="SIPServer1SwitchoverTimer" value="60" override="true"/>
    <setting id="TelephonyVmNumber1" value="" override="true"/>
    <setting id="SIPMessageWaitingIndicationUri1" value="" override="true"/>
    <!--Audio SIP account 1-->
    <setting id="AudioPayloadTypes1" value="101;96" override="true"/>
    <setting id="AudioVad1" value="false" override="true"/>
    <setting id="SIPPreferredVocoder1" value="0;8;18;9;98;125" override="true"/>
    <setting id="AudioPacketTime1" value="20;20;20;20;20;20" override="true"/>

    <!--Auto Answer account1-->
    <setting id="TelephonyInterphonyStatus1" value="false" override="true"/>

    <!--Intercom account1-->
    <setting id="SIPAutoAnsweredAllowed1" value="true" override="true"/>
    <setting id="SIPAutoAnsweredMute1" value="false" override="true"/>
    <setting id="SIPAutoAnsweredTone1" value="true" override="true"/>
    <setting id="SIPAutoAnsweredBarge1" value="false" override="true"/>
    <setting id="SIPGroup1IntercomType1" value="0" override="true"/>
<!--Dailing Rule Account 1-->
    <setting id="DialingRuleEnableHistory1" value="false" override="true"/>
    <setting id="DialingRuleEnableContact1" value="true" override="true"/>
    <setting id="DialingRuleEnableForward1" value="true" override="true"/>
    <setting id="DialingRuleEnableManual1" value="false" override="true"/>

 <!--custom mode account 1 -->
    <setting id="ForwardImmState1" value="false" override="true"/>
    <setting id="ForwardImmDest1" value="" override="true"/>
    <setting id="ForwardImmOnCode1" value="" override="true"/>
    <setting id="ForwardImmOffCode1" value="" override="true"/>
    <setting id="ForwardBusyState1" value="false" override="true"/>
    <setting id="ForwardBusyDest1" value="" override="true"/>
    <setting id="ForwardBusyOnCode1" value="" override="true"/>
<setting id="ForwardBusyOffCode1" value="" override="true"/>
    <setting id="ForwardNoReplyState1" value="false" override="true"/>
    <setting id="ForwardNoReplyDest1" value="" override="true"/>
    <setting id="ForwardNoReplyOnCode1" value="" override="true"/>
    <setting id="ForwardNoReplyOffCode1" value="" override="true"/>
```


12.1 SIP configuration file templates

The configuration file must be named as config.xxxxxxxxxxxx.xml, and xxxxxxxxxxxx is the mac address of the phone.

Note: Only Account1 configuration template involved in the following template. You can extend it to another 5 accounts as M Series DeskPhone supports 6 accounts.

```
<?xml version="1.0" encoding="UTF-8" ?>
 <settings>

                <!--SIP Parameters-->
                <setting id="SIPRegisterRetry" value="300" override="true"/>
                <setting id="SIPLocalSipPort" value="5060" override="true"/>
                <setting id="SIPLocalSipsPort" value="5061" override="true"/>
                <setting id="SIPLocalSrtpPort" value="30000" override="true"/>
                <setting id="SIPLocalSrtcpPort" value="30001" override="true"/>
                <setting id="SIPLocalRtpPort" value="6000" override="true"/>
                <setting id="SIPLocalRtcpPort" value="6001" override="true"/>

                <!--Audio-->
                <setting id="AudioToneCountry" value="1" override="true"/>
                <setting id="AudioDtmfFeedbackEnable" value="false" override="true"/>
                <setting id="AudioSidetoneHandset" value="0" override="true"/>
                <setting id="AudioHearingAidEnable" value="false" override="true"/>
                <setting id="Audiodiffserv" value="46" override="true"/>
                <setting id="AudioUseCustomTone" value="false" override="true"/>

                <!--Device Management Parameters-->
                <setting id="DmAdmcfgCfgfilePollingEnable" value="true" override="true"/>
                <setting id="DmAdmcfgCfgfilePollingTimeout" value="3600" override="true"/>
                <setting id="DmEnetcfgDns1" value="" override="true"/>
                <setting id="DmEnetcfgDns2" value="" override="true"/>
                <setting id="DmLldpcfgPowerPriority" value="2" override="true"/>
                <setting id="DmEnetcfgSntp" value="" override="true"/>
                <setting id="DmEnetcfgSntpRefreshPeriod" value="3600" override="true"/>
                <setting id="DmWpa802lxcfgMode" value="OFF" override="true"/>
                <setting id="DmSecucfgPcPort" value="true" override="true"/>
                <setting id="DmSecucfgPcPortVlanFilter" value="false" override="true"/>
            <setting id="DmSecucfgSsh" value="false" override="true"/>
                <setting id="DmAdminPasswd" value="123456" override="true"/>
                <setting id="DmSecucfgArpSpoofing" value="false" override="true"/>
                <setting id="DmSecucfgArpSpoofingTimer" value="500" override="true"/>

                <!--Firmware Upgrading-->
                <setting id="FirmwareUpdate" value="1" override="true"/>
                <setting id="DmEnetcfgUpgradeFile" value="" override="true"/>
                <setting id="DmAdmcfgUpdateTimeEnable" value="true" override="true"/>
                <setting id="DmAdmcfgUpdateTimeStart" value="04:00" override="true"/>
                <setting id="DmAdmcfgUpdateTimeDelta" value="5" override="true"/>

                <!--Dailing Rule-->
                <setting id="DialingToneEnabled" value="true" override="true"/>
                <setting id="Server1DialingRuleCountryCode" value="" override="true"/>
                <setting id="Server1DialingRuleAreaCode" value="" override="true"/>
                <setting id="Server1DialingRuleExternalPrefix" value="" override="true"/>
                <setting id="Server1DialingRuleMinNumberLength" value="" override="true"/>
             <setting id="Server1DialingRuleExternalPrefixExceptions" value="" override="true"/>

                <!--Forward setting -->
              <setting id="ForwardModeAccount" value="0" override="true"/>
              <setting id="TelephonyFwdMethod1" value="0" override="true"/>
            <!--phone mode -->
                <setting id="ForwardImmState" value="false" override="true"/>
                <setting id="ForwardImmDest" value="" override="true"/>
                <setting id="ForwardImmOnCode" value="" override="true"/>
                <setting id="ForwardImmOffCode" value="" override="true"/>
```

```
<setting id="PhoneProgKey12Label" value="" override="true"/>
<setting id="PhoneProgKey12Number" value="" override="true"/>
<setting id="PhoneProgKey12Extension" value="" override="true"/>
<setting id="PhoneProgKey13Type" value="" override="true"/>
<setting id="PhoneProgKey13Account" value="" override="true"/>
<setting id="PhoneProgKey13Label" value="" override="true"/>
<setting id="PhoneProgKey13Number" value="" override="true"/>
<setting id="PhoneProgKey13Extension" value="" override="true"/>
<setting id="PhoneProgKey14Type" value="" override="true"/>
<setting id="PhoneProgKey14Account" value="" override="true"/>
<setting id="PhoneProgKey14Label" value="" override="true"/>
<setting id="PhoneProgKey14Number" value="" override="true"/>
<setting id="PhoneProgKey14Extension" value="" override="true"/>
<setting id="PhoneProgKey15Type" value="" override="true"/>
<setting id="PhoneProgKey15Account" value="" override="true"/>
<setting id="PhoneProgKey15Label" value="" override="true"/>
<setting id="PhoneProgKey15Number" value="" override="true"/>
<setting id="PhoneProgKey15Extension" value="" override="true"/>
<setting id="PhoneProgKey16Type" value="" override="true"/>
<setting id="PhoneProgKey16Account" value="" override="true"/>
<setting id="PhoneProgKey16Label" value="" override="true"/>
<setting id="PhoneProgKey16Number" value="" override="true"/>
<setting id="PhoneProgKey16Extension" value="" override="true"/>
<setting id="PhoneProgKey17Type" value="" override="true"/>
<setting id="PhoneProgKey17Account" value="" override="true"/>
<setting id="PhoneProgKey17Label" value="" override="true"/>
<setting id="PhoneProgKey17Number" value="" override="true"/>
<setting id="PhoneProgKey17Extension" value="" override="true"/>
<setting id="PhoneProgKey18Type" value="" override="true"/>
<setting id="PhoneProgKey18Account" value="" override="true"/>
<setting id="PhoneProgKey18Label" value="" override="true"/>
<setting id="PhoneProgKey18Number" value="" override="true"/>
<setting id="PhoneProgKey18Extension" value="" override="true"/>
<setting id="PhoneProgKey19Type" value="" override="true"/>
<setting id="PhoneProgKey19Account" value="" override="true"/>
<setting id="PhoneProgKey19Label" value="" override="true"/>
<setting id="PhoneProgKey19Number" value="" override="true"/>
<setting id="PhoneProgKey19Extension" value="" override="true"/>
<setting id="PhoneProgKey20Type" value="" override="true"/>
<setting id="PhoneProgKey20Account" value="" override="true"/>
<setting id="PhoneProgKey20Label" value="" override="true"/>
<setting id="PhoneProgKey20Number" value="" override="true"/>
<setting id="PhoneProgKey20Extension" value="" override="true"/>

<!--M3 Modle phones can't support below parameters of program key 21-28-->

<setting id="PhoneProgKey21Type" value="" override="true"/>
<setting id="PhoneProgKey21Account" value="" override="true"/>
<setting id="PhoneProgKey21Label" value="" override="true"/>
<setting id="PhoneProgKey21Number" value="" override="true"/>
<setting id="PhoneProgKey21Extension" value="" override="true"/>
<setting id="PhoneProgKey22Type" value="" override="true"/>
<setting id="PhoneProgKey22Account" value="" override="true"/>
<setting id="PhoneProgKey22Label" value="" override="true"/>
<setting id="PhoneProgKey22Number" value="" override="true"/>
<setting id="PhoneProgKey22Extension" value="" override="true"/>
<setting id="PhoneProgKey23Type" value="" override="true"/>
<setting id="PhoneProgKey23Account" value="" override="true"/>
<setting id="PhoneProgKey23Label" value="" override="true"/>
<setting id="PhoneProgKey23Number" value="" override="true"/>
<setting id="PhoneProgKey23Extension" value="" override="true"/>
<setting id="PhoneProgKey24Type" value="" override="true"/>
<setting id="PhoneProgKey24Account" value="" override="true"/>
<setting id="PhoneProgKey24Label" value="" override="true"/>
<setting id="PhoneProgKey24Number" value="" override="true"/>
<setting id="PhoneProgKey24Extension" value="" override="true"/>
<setting id="PhoneProgKey25Type" value="" override="true"/>
<setting id="PhoneProgKey25Account" value="" override="true"/>
<setting id="PhoneProgKey25Label" value="" override="true"/>
<setting id="PhoneProgKey25Number" value="" override="true"/>
<setting id="PhoneProgKey25Extension" value="" override="true"/>
<setting id="PhoneProgKey26Type" value="" override="true"/>
<setting id="PhoneProgKey26Account" value="" override="true"/>
<setting id="PhoneProgKey26Label" value="" override="true"/>
<setting id="PhoneProgKey26Number" value="" override="true"/>
<setting id="PhoneProgKey26Extension" value="" override="true"/>
<setting id="PhoneProgKey27Type" value="" override="true"/>
```

112


```
<!--custom mode account 1-->
    <setting id="TelephonyDndState1" value="false" override="true"/>
    <setting id="TelephonyDndOnCode1" value="" override="true"/>
    <setting id="TelephonyDndOffCode1" value="" override="true"/>
 <!--LDAP-->
<setting id="LDAPEnabled" value="true" override="true"/>
<setting id="LDAPFieldsMapping" value="{ &quot;firstname&quot; :
&quot;givenname&quot;, &quot;name&quot; : &quot;sn&quot;, &quot;officephone&quot; :
&quot;telephonenumber&quot;}" override="true"/>
<setting id="LDAPLogin" value="default" override="true"/>
<setting id="LDAPPassword" value="default" override="true"/>
<setting id="LDAPServerUrl" value="" override="true"/>
<setting id="LDAPFilter" value="(|(givenname=*%1*)(sn=*%1*))" override="true"/>
<setting id="LDAPSearchBase" value="o=ALE,o=directoryRoot" override="true"/>

    <!--BLF resource list setting-->
    <setting id="BLFListInitPosType" value="" override="true"/>

    <!--Programm key-->
    <setting id="PhoneProgKey1Type" value="" override="true"/>
    <setting id="PhoneProgKey1Account" value="" override="true"/>
    <setting id="PhoneProgKey1Label" value="" override="true"/>
    <setting id="PhoneProgKey1Number" value="" override="true"/>
    <setting id="PhoneProgKey1Extension" value="" override="true"/>
    <setting id="PhoneProgKey2Type" value="" override="true"/>
    <setting id="PhoneProgKey2Account" value="" override="true"/>
    <setting id="PhoneProgKey2Label" value="" override="true"/>
    <setting id="PhoneProgKey2Number" value="" override="true"/>
    <setting id="PhoneProgKey2Extension" value="" override="true"/>
    <setting id="PhoneProgKey3Type" value="" override="true"/>
    <setting id="PhoneProgKey3Account" value="" override="true"/>
    <setting id="PhoneProgKey3Label" value="" override="true"/>
    <setting id="PhoneProgKey3Number" value="" override="true"/>
    <setting id="PhoneProgKey3Extension" value="" override="true"/>
    <setting id="PhoneProgKey4Type" value="" override="true"/>
    <setting id="PhoneProgKey4Account" value="" override="true"/>
    <setting id="PhoneProgKey4Label" value="" override="true"/>
    <setting id="PhoneProgKey4Number" value="" override="true"/>
    <setting id="PhoneProgKey4Extension" value="" override="true"/>
    <setting id="PhoneProgKey5Type" value="" override="true"/>
    <setting id="PhoneProgKey5Account" value="" override="true"/>
    <setting id="PhoneProgKey5Label" value="" override="true"/>
    <setting id="PhoneProgKey5Number" value="" override="true"/>
    <setting id="PhoneProgKey5Extension" value="" override="true"/>
    <setting id="PhoneProgKey6Type" value="" override="true"/>
     <setting id="PhoneProgKey6Account" value="" override="true"/>
    <setting id="PhoneProgKey6Label" value="" override="true"/>
    <setting id="PhoneProgKey6Number" value="" override="true"/>
    <setting id="PhoneProgKey6Extension" value="" override="true"/>
    <setting id="PhoneProgKey7Type" value="" override="true"/>
    <setting id="PhoneProgKey7Account" value="" override="true"/>
    <setting id="PhoneProgKey7Label" value="" override="true"/>
    <setting id="PhoneProgKey7Number" value="" override="true"/>
    <setting id="PhoneProgKey7Extension" value="" override="true"/>
    <setting id="PhoneProgKey8Type" value="" override="true"/>
    <setting id="PhoneProgKey8Account" value="" override="true"/>
    <setting id="PhoneProgKey8Label" value="" override="true"/>
    <setting id="PhoneProgKey8Number" value="" override="true"/>
    <setting id="PhoneProgKey8Extension" value="" override="true"/>
    <setting id="PhoneProgKey9Type" value="" override="true"/>
    <setting id="PhoneProgKey9Account" value="" override="true"/>
    <setting id="PhoneProgKey9Label" value="" override="true"/>
    <setting id="PhoneProgKey9Number" value="" override="true"/>
    <setting id="PhoneProgKey9Extension" value="" override="true"/>
    <setting id="PhoneProgKey10Type" value="" override="true"/>
    <setting id="PhoneProgKey10Account" value="" override="true"/>
    <setting id="PhoneProgKey10Label" value="" override="true"/>
    <setting id="PhoneProgKey10Number" value="" override="true"/>
    <setting id="PhoneProgKey10Extension" value="" override="true"/>
    <setting id="PhoneProgKey11Type" value="" override="true"/>
    <setting id="PhoneProgKey11Account" value="" override="true"/>
    <setting id="PhoneProgKey11Label" value="" override="true"/>
    <setting id="PhoneProgKey11Number" value="" override="true"/>
    <setting id="PhoneProgKey11Extension" value="" override="true"/>
    <setting id="PhoneProgKey12Type" value="" override="true"/>
    <setting id="PhoneProgKey12Account" value="" override="true"/>
```

12.2.2 SIP servers/groups/accounts

Note:

SIP Group1/Server1 is mandatory for the main SIP server (other groups are not described in this document)

Parameter	Default	Value range	Mandatory	Description
SIPServer1Address			Y	SIP Server1 address
SIPServer1Port	5060	0-65535	N	SIP Server1 port number for registration
SIPServer1GroupNumber	1	1-4	N	Group number of this SIP Server1
SIPGroup1ServerType	0	0:Default 4:swyx 5:uaCSTA 6:BroadSoft 7:Asterisk 8:3cx 9:SIPWISE 10:MetaSwitch	N	Server type for group1 Note: DO NOT USE 1,2,3 which are ALEInternational solutions
SIPGroup1DomainName			N	Group1 SIP server domain name
SIPGroup1AuthenticationRealm			N	Group1 SIP authentication realm
SIPGroup1AuthenticationName			N	Group1 SIP authenticate name Mandatory if SIP server requests authentication
SIPGroup1AuthenticationPassword			N	Group1 SIP authenticate password Mandatory if SIP server requests authentication
SIPGroup1DisplayName			N	Group1's display name
SIPGroup1DtmfMode	2	0:None 1:InBand 2:RFC2833 3:RFC4733 4:SIP_INFO 5:SIP_INFO +RFC2833		Defines the DTMF mode
SIPGroup1DeviceUri			Y	Group1's device URL used for registration

12.2.3 Outbound proxy

In some network topologies, outbound proxy will be used for SIP registration. The related parameters to be used in the case are listed below.

Parameter	Default	Value range	Mandatory	Description
SIPGroup1OutBoundProxyAddress			N	Outbound proxy address for group1
SIPGroup1OutBoundProxyPort	5060	0-65535	N	Outbound proxy port for group1 *Note:* *The DNS SRV will be enabled while set port 0 with valid outbound proxy.*


```
                    <setting id="PhoneProgKey27Account" value="" override="true"/>
                    <setting id="PhoneProgKey27Label" value="" override="true"/>
                    <setting id="PhoneProgKey27Number" value="" override="true"/>
                    <setting id="PhoneProgKey27Extension" value="" override="true"/>
                    <setting id="PhoneProgKey28Type" value="" override="true"/>
                    <setting id="PhoneProgKey28Account" value="" override="true"/>
                    <setting id="PhoneProgKey28Label" value="" override="true"/>
                    <setting id="PhoneProgKey28Number" value="" override="true"/>
                    <setting id="PhoneProgKey28Extension" value="" override="true"/>
</settings>
```

12.2 Description of the SIP settings in configuration file

Sections below give a description for the main SIP settings in the configuration file. The list of settings is not exhaustive.

12.2.1 Firmware upgrading

Parameter	Default	Value range	Mandatory	Description
DmEnetcfgUpgradeFile			N	Downloading URL for firmware binary files
DmAdmcfgUpdateTimeEnable	false	true; false	N	True: the phone will check the binary version. If different from current version, the upgrading process will be triggered. False: the phone will not check the binary information any more.
DmAdmcfgUpdateTimeStart	00:00		N	Defines when the phone will check if the binary has changed during the last 24 hours. Time format supported: HH:MM
DmAdmcfgUpdateTimeDelta	0	[0,1440]		In order to prevent all terminals from starting an upgrade at the same time, this setting will add a random value between 0 and 1440 min before the value defined with DmAdmcfgUpdateTime Start. In this way, upgrade parameters can be configured with the same values for all sets, but each sets will update at different time.

		+3:30 +4:00 +4:30 +5:00 +5:30 +5:45 +6:00 +6:30 +7:00 +8:00 +8:45 +9:00 +9:30 +10:00 +10:30 +11:00 +11:30 +12:00 +12:45 +13:00 +13:30 +14:00		
DmAdmcfgTimeZoneLocation				Country or area name of time zone, useful when DST enable is auto
DmAdmcfgDstEnable	0	0,1		0 is disable, 1 is enable
DmAdmcfgDstType	week	Week date		DST is set by week or by date
DmAdmcfgDstStartMonth	Jan	Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec		
DmAdmcfgDstStartWeek	5	1,2,3,4,5		1 is first, 2 is second, 3 is third, 4 is fourth, 5 is last
DmAdmcfgDstStartDate	1			
DmAdmcfgDstStartHour	0	[0,23]		
DmAdmcfgDstEndMonth	Dec	Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec		
DmAdmcfgDstEndWeek	5	1,2,3,4,5		1 is first, 2 is second, 3 is third, 4 is fourth, 5 is last
DmAdmcfgDstEndDate	30			
DmAdmcfgDstEndHour	23	[0,23]		
DmAdmcfgDstOffset	60	[-300,300]		Offset time when DST is on, in minutes

12.2.7 Customized logo of screensaver

Parameter	Default	Value range	Mandatory	Description
ScreensaverLogoURL			N	URL for download the customized Logo of screen saver

12.2.4 SIP-TLS/SRTP

To deploy the phone to be working in SIP-TLS & SRTP mode, below parameters should be configured in that sip Group.

Parameter	Default	Value range	Mandatory	Description
SIPGroup1TransportMode	0	0:UDP 1:TCP 2:TLS	N	Protocol used on transport layer for server group1
SIPGroup1SrtpWorkingMode	0	0:none 1:Best effort 2:Strict	N	SRTP mode used on transport layer for server group1
SIPCertificateUrl			N	URL for download the SIP server certificate
SIPSslPeerVerify	false	true false	N	Whether to enable the peer verify for SIPs
SIPSslVersion	0	0: All 1: TLS1.0 2: TLS1.2	N	SSL version supported by terminal

12.2.5 Management of SSL connection

Parameter	Default	Value range	Mandatory	Description
DmSecucfgSsh	false	true false	N	Enables SSH connections
DmAdminPasswd			N	Used to set password for the user **admin**

12.2.6 SNTP&Timezone

Parameter	Default	Value range	Mandatory	Description
DmEnetcfgSntp			N	SNTP Server
DmAdmcfgTimeZoneUtoffset		-11:00 -10:00 -9:30 -9:00 -8:00 -7:00 -6:00 -5:00 -4:30 -4:00 -3:30 -3:00 -2:30 -2:00 -1:00 0 +1:00 +2:00 +3:00		Offset time from UTC time

12.2.8 LDAP

Parameter	Default	Value range	Mandatory	Description
PhoneProgKey[1,28]Type	0	0 - Not Used 1 - Speed Dial 59 - BLF 2 - BLF List 3 - Do Not Disturb 4 - Directory 5 - VoiceMail 6 - Conference 7 - Forward 8 - Transfer 9 - Group Listening 10 - HeadSet 11 - Hot Desking 12 - Phone Lock 13 - Prefix 14 - DTMF 15 - Direct Pickup 16 - Group Pickup 17 - Call Park 18 - Recall 19 - XML Browser 21 - Intercom 23 - AudioHub 58 - Hold 60 - Account	N	The type of phone program key
PhoneProgKey[1,28]Account	1	1-8	N	The account index of phone program key. 1: Account 1 2: Account 2 3: Account 3 4: Account 4 5: Account 5 6: Account 6 7: Account 7 8: Account 8
PhoneProgKey[1,28]Label			N	The label of phone program key
PhoneProgKey[1,28]Number			N	The number of phone program key
PhoneProgKey[1,28]Extension			N	The extension of phone program key

END OF DOCUMENT

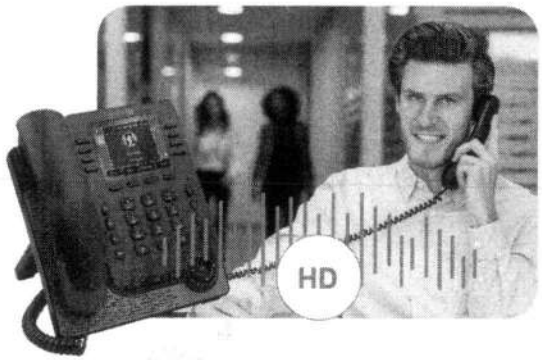
Enhanced HD Voice, Exceptional 360° Audio Tuning

Enhanced HD Voice
The Myriad Series offers first-class HD audio performance with enhanced audio components and sound chamber design. Super wideband in handsfree mode delivers Symphonic HD Voice that takes audio experiences to the next level.

360° Audio Tuning
The Myriad Series features exceptional 360° audio tuning around the phone in handsfree mode. Together with super wideband technology and the full-duplex speakerphone, it makes the phone an excellent hands-free conference speaker for 3-4 people.

Symphonic HD

360°



Classic Elegant Design, Enhanced User Experience

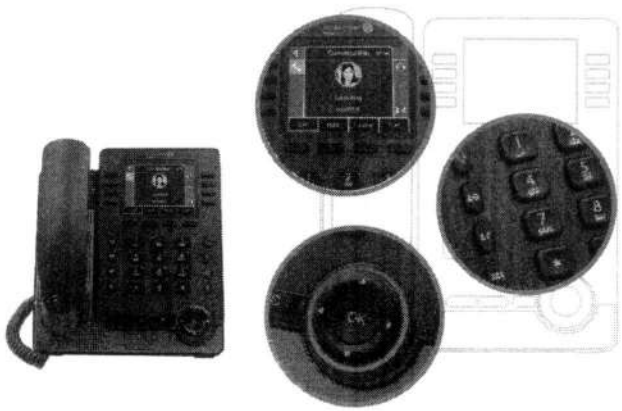
The Myriad Series has an elegant, sleek industrial design inspired by the Eiffel Tower. The modern, intuitive user interface enables easy call management and quick access to up to 8 lines. It features large hard keys, vivid LED indicators and a 4-way navigator centered with the "OK" key for an enhanced user experience.

The M5 and M7 phones include colour displays, further boosting operation efficiency. In addition, the phones have the optional capability of faceplate customization to further improve brand presence.

Colour Display

Elegant Design

Intuitive UI



Myriad Series Enterprise-Grade Desktop IP Phone

ALE's latest Myriad Series includes 3 enterprise-class SIP phone models, the M3, M5, and M7, suitable for executives, managers, and professionals with a high demand for quality telephony services.

The Myriad Series delivers outstanding performance with enhanced HD audio quality, a modern intuitive user interface, and enhanced telephony features. It enables users to easily manage their calls, enjoy a smooth user experience and ultimately improve productivity.

MYRIAD

Alcatel-Lucent Enterprise



Model	M7	M5	M3
LCD Size (screen)	3.5", 320x240-pixel	2.8", 320x240-pixel	2.8", 128x64-pixel
LCD Type	Colour, backlit		Black & white, backlit
USB Port	2 (Type A & Type C)		
POE	Class 2		
Ethernet Port	2x10/100M/1000M		
External PA Port	USB Type C		
External Headset Port	USB Type A/C		
Bluetooth	Yes	No	
WiFi Dongle	Yes		
Expansion Module	EM20/EM200		
Line (SIP Account)	8		
Audio Codec	G.711/G.729/G.722/OPUS/iLBC		
Super Wideband	Yes, in hands-free mode		
Contact/Call Log	1,000 records		
VPN	OpenVPN		
Security	SIP TLS, SRTP, 802.1x, AES-256		
Provisioning	HTTP/HTTPS, TR069, ALE EDS/EPS		

Contact us: www.aledevice.com www.al-enterprise.com

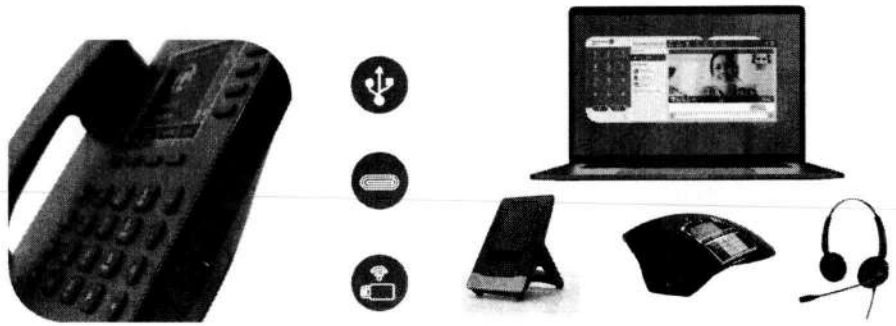
Alcatel-Lucent Enterprise

Advanced Connectivity (Audio Hub), Great Flexibility

The Myriad Series can connect to PC softphone calls through an integrated USB port, turning the deskphone into an Audio Hub. This turns the deskphone into a high-quality speakerphone that can stream audio in enhanced HD or a full duplex handsfree device.

The series also supports connection to external devices such as ALE expansion modules (EM20/EM200), Wi-Fi dongles, and wired or wireless Bluetooth headsets, allowing customers to best leverage the value of their phones.

The USB-C port can also be used to power deskphones like most smartphones on the market.

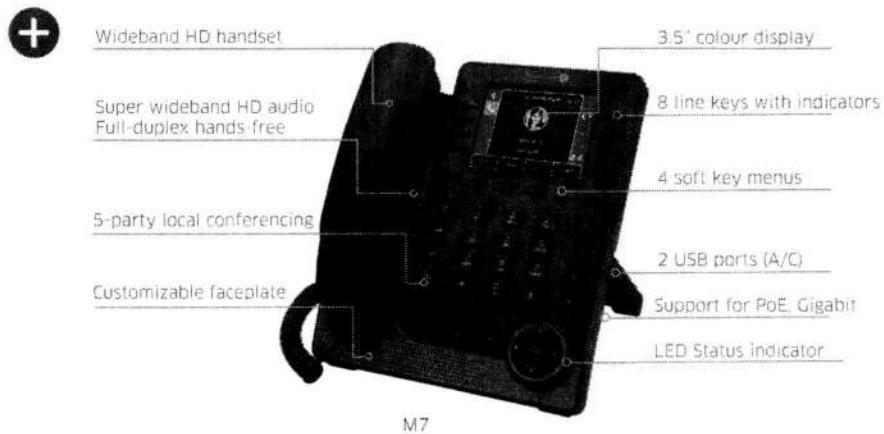


Expansion Module External Speaker Headset

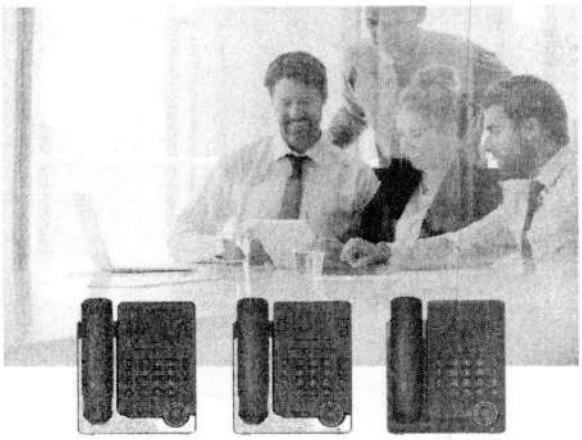
Enterprise-grade Functionality, Seamless Platform integration

The Myriad Series offers enterprise-grade telephony features such 8 line keys, 4 programmable soft keys, Gigabit support and 5-party local conferencing to better facilitate business efficiency and boost teamwork.

The standard SIP protocol offers seamless integration with major open SIP servers such as Asterisk, BroadSoft, Metaswitch, and Nfon.



M7



M7 DeskPhone
M5 DeskPhone
M3 DeskPhone

User Manual

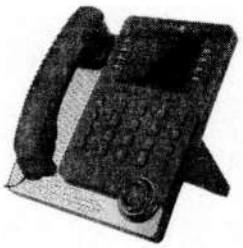
8AL90382ENAAed02
06/2020

Alcatel·Lucent Enterprise

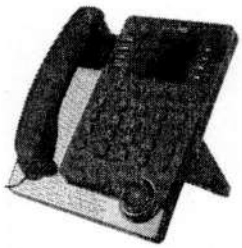
Introduction

Thank you for choosing an Alcatel-Lucent phone.

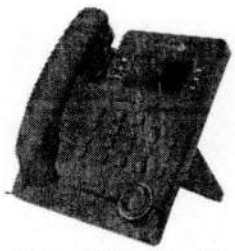
This document describes the services offered by the M3, M5 and M7 DeskPhones connected to a SIP server.



Alcatel-Lucent M7 DeskPhone (M7).



Alcatel-Lucent M5 DeskPhone (M5).



Alcatel-Lucent M3 DeskPhone (M3).

The phones described in this document are supported on different SIP servers, and some features described in this document depend on the SIP server to which the phone is connected.
If more information about system compatibility or about the level of features for a given SIP server is needed, please contact your system administrator.

The labels and icons displayed depend on the type and the skin of the set. The label is not displayed if the corresponding feature is not configured on your telephone system. Depending on the size of the display, some labels may be truncated. *All labels are displayed in color and are italicized.* This icon describes a succession of actions or labels you have to do or select: →.
This icon describes the consequence of an action: ››.

Some features depend on the type of the set.

	M7	M5	M3
IP Phone	●	●	●
Multiple SIP Accounts	●	●	●
Color screen	●	●	
Monochrome screen			●
Bluetooth® Smart Ready	●		
ompatible with Bluetooth ® headset	●		
USB headset	●	●	●
Wi-Fi dongle compatible*	●	●	●
Two-port Gigabit Ethernet switch with Power Over Ethernet support	●	●	●
Add-on module EM20	●	●	●
Add-on module EM200	●	●	●
Audio services (hands-free, handset and headset)	●	●	●
Adjust the brightness of the display	●	●	●
Local conference	●	●	●
Peer to peer SIP calls	●	●	●
Web Management	●	●	●
Desk sharing	●	●	●
Teleworking (OpenVPN)	●	●	●

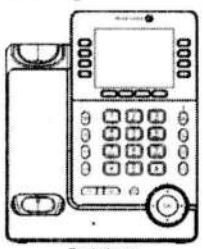
*To know the supported dongle, please refer to the Alcatel-Lucent Enterprise website or contact your administrator.

The labels and icons presented in this document are not contractually binding and may be modified without prior warning.

118

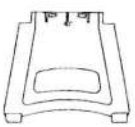
1 Getting started

1.1 Unboxing



Deskphone

Handset



2-degree adjustable foot

Handset cord

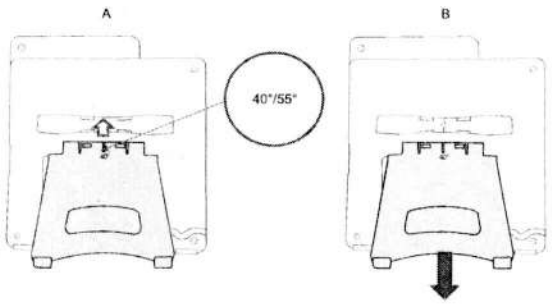
Ethernet cable

Safety and regulatory instructions

1.2 Install your desk phone

1.2.1 Install the foot

Clip the foot into its compartment behind the phone. Your desk phone provides a 2-degree foot. Depending on the way you insert the foot into the phone, your desk phone will have a different angle: 55° or 40°. The angle noted on the top of the foot (face up) corresponds to the angle that the phone will have after having inserted the foot.



To unclip the foot, pull it straight back until it separates from the phone.

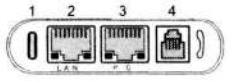
119

1.2.2 Connect the device

Please read safety instructions first.

Connect the handset (4) if it is not connected (your phone is usually provided with the handset connected).

If your desk phone is correctly configured, you can connect it to the network (2). If your desk phone is not powered by PoE (Power over Ethernet), you have to plug the power adapter to the USB-C connector (1) and connect it to the AC power supply. The power adapter is sold separately. For more information, contact your installer or administrator.



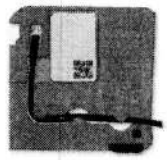
For more details, please consult the section: Description of the connectors.

1.2.3 Install a comfort wired handset

Your phone is provided with a connected handset.

If you have to replace it:

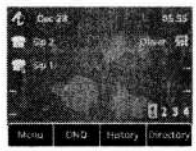
- Plug-in the wired handset to the appropriate connector (refer to phone description).
- Make sure you position the cable correctly in the compartment intended for that purpose.



1.3 Multiple SIP accounts

Your phone supports multiple SIP accounts. Your administrator can declare up to 4 SIP accounts. A default account is used for calls unless you select the relevant account prior the call. When you have programmed some function keys, you can associate a SIP account to the key.

It is recommended to program a key for each SIP account in the main page, as a line key. Then the status of the account is displayed on the homepage. The key of the SIP account receiving an incoming call is blinking.



	If the homepage displays an SIP account (line key), select the SIP account to use in order to make the call.
	The default SIP account is marked by a green point.
	Forward is activated for this account.
	Do not Disturb is activated for this account.

The call log lists all incoming and outgoing calls for all SIP accounts. The concerned SIP account is displayed by opening the details of the call log entry.

1.3.1 Program a line key for a SIP account

	Long press on a programmable key.
Switch or	Define the type of programmable key: *Account* Select the relevant account. Add a label.
or *Save*	Save the programmable key.

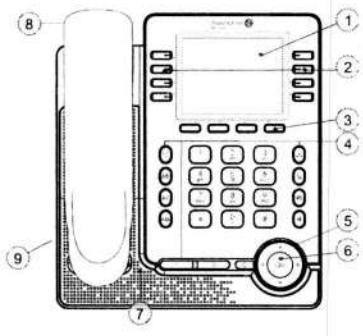
1.3.2 Define the default SIP account

	The phone is in idle state.
Menu	Press the Menu soft key to access the Main Menu.
Features	Use up-down and 'ok' navigation keys to select: *Features*.
Default Account	Use up-down and 'ok' navigation keys to select: *Default Account*.
Switch or	Select the default SIP account.
or *Save*	Validate your choice.
	To end the settings.

2 Getting to know your telephone

2.1 M7 DeskPhone

This phone is part of the IP phone range. With its color display associated to 12 dedicated functions keys, and an intuitive navigation key, the M7 DeskPhone delivers excellent user experience and optimum conversation convenience with outstanding audio quality in either hands-free mode or when using the comfort handset. It is 'Bluetooth® Smart Ready'. Your phone is very easy to use thanks to its natural perception user interface. Your experience is further enhanced with Bluetooth® accessories. It is compatible with remote working. By this way, it is perfect for use at your office in your enterprise or at home (remote working).



1	3.5 inch color display.	6	Navigation.
2	28 programmed keys: SIP account, speed dial, functions. Use navigation keys to navigate through pages of programmable keys.	7	• Super wideband loudspeaker for optimized sound. • Microphone.
3	Softkeys: menus and actions available depending on the selected page. Softkeys are configurable by the administrator. • Idle state: menu to access features and configure the phone or manage calls. Use the navigation keys to navigate through the menus. • In conversation: available actions.	8	Wired handset (wide band audio quality).
4	Permanent feature keys: quick access to the phone's main features.	9	2-degree adjustable foot (55°,40°).
5	LED Flashing blue: incoming calls, new events displayed on the screen (voice messages, missed calls). Blue steady: ongoing call.		

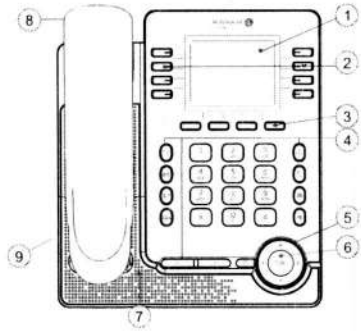
2.1.1 Bluetooth® Smart Ready

Bluetooth Your phone is 'Bluetooth® Smart Ready'. It can receive and share Bluetooth® signals from various Bluetooth® devices (Bluetooth® and Bluetooth® Smart or Low-energy devices). It is ready for future services available on the fly in a subsequent software upgrade. This feature can be deactivated by the administrator.

120

2.2 M5 DeskPhone

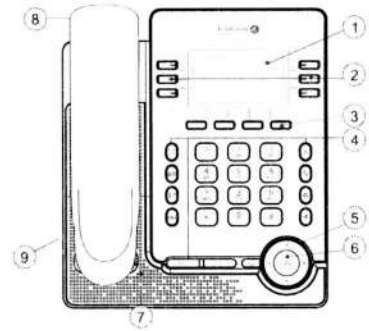
This phone is part of the IP phone range. In addition to a color display associated to 12 dedicated function keys and an intuitive navigation key, the M5 DeskPhone delivers excellent user experience and optimum conversation convenience with an outstanding audio quality in either hands-free mode or when using the comfort handset. Your phone is very easy to use thanks to its natural perception user interface. It is compatible with remote working. By this way, it is perfect for use at your office in your enterprise or at home (remote working).



1	2.8 inch color display.	6	Navigation.
2	28 programmed keys: SIP account, speed dial, functions. Use navigation keys to navigate through pages of programmable keys.	7	• Super wideband loudspeaker for optimized sound. • Microphone.
3	Softkeys: menus and actions available depending on the selected page. Softkeys are configurable by the administrator. • Idle state: menu to access features and configure the phone or manage calls. Use the navigation keys to navigate through the menus. • In conversation: available actions	8	Wired handset (wide band audio quality).
4	• Permanent feature keys: quick access to the phone's main features.	9	2-degree adjustable foot (55°,40°).
5	LED Flashing blue: incoming calls, new events displayed on the screen (voice messages, missed calls). Blue steady: ongoing call.		

2.3 M3 DeskPhone

This phone is part of the IP phone range. In addition to a clear monochrome display associated to 10 dedicated function keys and an intuitive navigation key, the M3 DeskPhone provides high audio fidelity for telephone calls either in hands-free mode or when using the comfort handset. Your phone is very easy to use thanks to its natural perception user interface. It is compatible with remote working. By this way, it is perfect for use at your office in your enterprise or at home (remote working).

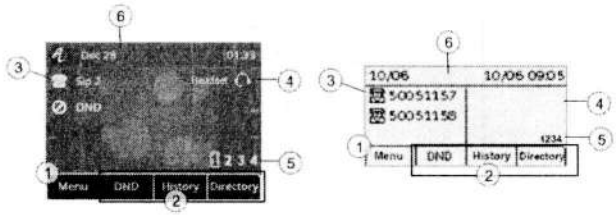


1	2.8 inch monochrome display.	6	Navigation.
2	20 programmed keys: SIP account, speed dial, functions. Use navigation keys to navigate through pages of programmable keys.	7	• Super wideband loudspeaker for optimized sound. • Microphone.
3	Softkeys: menus and actions available depending on the selected page. Softkeys are configurable by the administrator. • Idle state: menu to access features and configure the phone or manage calls. Use the navigation keys to navigate through the menus. • In conversation: available actions.	8	Wired handset (wide band audio quality).
4	Permanent feature keys: quick access to the phone's main features.	9	2-degree adjustable foot (55°,40°).
5	LED Flashing blue: incoming calls, new events displayed on the screen (voice messages, missed calls). Blue steady: ongoing call.		

2.4 Main screen

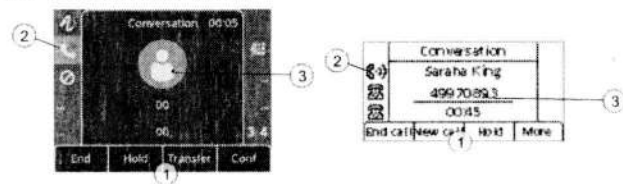
Your phone can support up to 4 SIP accounts.

The main screen, composed with 4 pages, displays all programmed keys which can be a line key for a registered SIP account, a speed dial or other functions.



1	Menu to access features and configure the phone or manage calls. Press the menu softkeys under the screen to access features. Use the up-down navigation keys to navigate through the menus and to select an entry or an option.
2	3 dynamic keys configurable by your administrator to access features of the phone.
3	Line keys associated with SIP account (optional). Press the line key associated with a SIP account to make a call with this account or to answer an incoming call to this account.
4	Programmed keys. Press the programmed key to use the programmed function or contact. Long press the programmed key to enter into the key configuration. The 'headset' programmed key allows you to switch to headset mode.
5	Access to 4 pages. Use the right-left navigation keys or the '1234' programmed key to navigate between pages. The number of the displayed page is highlighted.
6	Date, time and status bar.

2.5 Call management screen



1	Softkeys: actions available depending on the call status. Press the softkey under the label to select the corresponding feature.
2	SIP account in conversation.
3	Incoming call and conversation presentation screen.

2.6 Navigation keys

	OK key: Use this key to validate your choices and options while programming or configuring (short press). **left-right navigator:** Use to move from one page to another or to move the cursor in a text box. **up-down navigator:** Use to select an item on a list. When information extends over more than one page, use the down navigation key to display the next page. Use the up navigation key to display the previous page.
C	**Back/Exit key:** Use this key to go back to the previous step.
Bkspc	Use this key to delete the previous input letter or number in the text box.
More	Open other functions.

Use the up-down navigation keys to navigate through the menus and to select an entry or an option.

121

2.7 Permanent features keys

- Take the call key.
- Redialing the last number dialed (long press).
- List of last numbers dialed (short press).

- Placing a call on hold.
- Recover the call on hold.

- Transfer a call.

- Starting a conference call with two contacts.

- Reject incoming call.
- Hang up.
- Return to the main page.

- Mute key
  During a call, press this key to stop your contact from hearing you. When activated, the key is lit red.

- Access the voice mail
  The message key flashes red when you have received a new voicemail or a missed an incoming call. The key stays on if there are old messages in the voicemail box.

- Press this key to open dialer in hands-free mode (idle state).
- Pressing this key answers an incoming call in hands-free mode (idle state). When a call is in progress, pressing this key switches from hands-free mode to headset or handset mode. When activated, the key is lit blue.
- Hang up in hands-free mode if the headset mode is not activated.

- Decrease the volume of the ring tone (9 steps) in idle state or when you receive an incoming call.
- Decrease the volume of the handset, loudspeaker or headset (7 steps) during a conversation.

- Increase the volume of the ring tone (9 steps) in idle state or when you receive an incoming call.
- Increase the volume of the handset, loudspeaker or headset (7 steps) during a conversation.

2.8 Programmed key icons

This table lists icons displayed on the screen when you program a key. To program a key, see chapter: Programmable keys. The following icons are listed when the phone is in an idle state and can be changed depending on the status of the phone or the contact's phone.

- SIP account.
- Speed dial.
- BLF/BLF List (Busy Lamp Field).
- Hold.
- Transfer.
- Conference.
- Recall the last number.
- Do not disturb.
- Directory.
- Forward.
- Voicemail.
- Hot Desking.
- Prefix.
- DTMF Tone.
- Direct pick up.
- Group pick up.
- Headset.
- Group Listen.
- Intercom.
- Audio Hub.
- XML Browser.
- Phone Lock.

2.9 Status icons/ Call icons

Icons providing information about certain specific configurations on the phone or about the call status.

Status icons

Depending on the size of the display, all status icons may not be displayed simultaneously. Which icons are displayed depends on their priority. The following icons are listed according to their priority, from the highest to the lowest.

Status icons are displayed in the top bar of the screen.

- Silent mode.
- Telephone locked.
- Headset connected.
- Handsfree connected.
- Bluetooth ® accessory paired.
- Wi-Fi enabled.
- Interphony mode (Auto answer).
- Do not disturb.
- Audio Hub: PC not connected.
- Audio Hub: PC not connected.
- Updating in progress.

The call status is also displayed at the top of the call management screen:

- *Dial*: dial number.
- *Ringing*: Incoming calls.
- *Conversation*: In conversation.
- *On hold*: During a conversation, the contact is on hold.
- *Conference*: Conference mode with 2 contacts.

Call icons

Call icons are associated to a SIP account and are displayed at the level of the line key programmed in the home page. A text with call status is displayed in the top of the incoming call/conversation presentation screen.

- SIP account (idle state). A grayed or crossed icon means that the SIP account is not registered (Please contact your administrator).
  Line keys.
- Incoming call icon.
- Call in progress icon.
- Call on hold icon.

2.10 Alpha-numeric keyboard

Your phone is equipped with alphanumeric keyboard. You can switch between numeric keyboard to dial number, and alphabetic keyboard to enter text by pressing the corresponding preprogrammed key.

- Switch between the alphabetic and numeric keyboards:

abc	When you are in a text zone, you can switch to the alphabetic keyboard by selecting this key.
123	When alphabetic keyboard is activated, select this key to switch to the numeric keyboard.

- Enter alphabetic characters.
  The number pad keys have letters that you can display by successive presses. The number is the last character in the series. Some special characters can be displayed by successively pressing the key:

	% $ / ~ & ( ) [ ] = *
	@ #
	space - _ 1
	+ . , ; : / \ ? ! 0

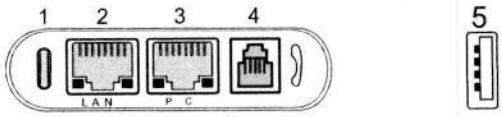
- Use navigation keys to move the cursor into the text.
- *Bkspc* Use this key to delete the last entered character. The alphabetic mode remains activated.

122

2.11 Description of the connectors

Various connections to allow phone extensions. The type of connectors you have depends on your phone.

M7, M5, M3



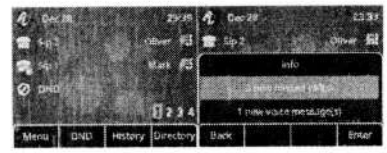
		M7	M5	M3
1	Universal Serial Bus (USB-C) connector This connector is used for: • Connect the power adapter. • Connect a headset. • Connect a PC to use the desk phone as an audio hub.	●	●	●
2	10/100/1000 Mbps Ethernet connectors to the enterprise network (LAN - RJ45).	●	●	●
3	10/100/1000 Mbps Ethernet connectors to a PC (RJ45).	●	●	●
4	Wired handset connector (RJ9).	●	●	●
5	Universal Serial Bus (USB-a) connector. This connector is used for: • Connect a USB headset. • Connect an add-on module. • Connect a Wi-Fi dongle*. • Connect a PC to use the desk phone as an audio hub.	●	●	●

*To know the supported dongle, please refer to the Alcatel-Lucent Enterprise website or contact your administrator.

3 Using your telephone

3.1 Information about the phone

The main page can display all SIP accounts used on the phone and other programmed keys. For each SIP account used on the phone, we recommend creating a programmed key to obtain information about account status. The icon associated to a SIP account provides the status of the account.



Information about new events such as missed calls and new voice message(s) are displayed in a pop-up on the main page. The message key flashes red when you have received a new voicemail or a missed an incoming call. When the new events pop-up is displayed, the blue LED of the phone flashes slowly.

3.1.1 More information about new events

	If the new events pop-up is not displayed, click on the message key to open it.
	Select the event to consult.
or *Enter*	

3.2 Making call

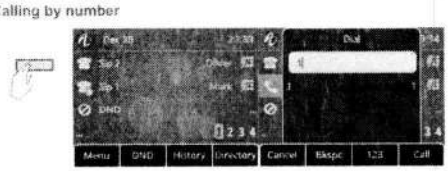
3.2.1 Open the dialer

This section describes how to make a call. There are different ways to open the dialer before calling your contact.

Use one of the following:	
	Dial directly the number for your call.
	Unhook the handset or the headset.
	Press the 'take the call' key.
	Press the loudspeaker/hands-free key.
	If the homepage displays an SIP account (line key), select the SIP account to use in order to make the call. This key has to be programmed in the homepage.

You can unhook the handset or the headset to make a call with the handset or the headset otherwise you make a call in hands-free mode.

3.2.2 Calling by number



	Open the dialer.
Use one of the following:	
	Dial the number.
	Select the contact to call in the list of last number dialed.
Use one of the following:	
	Press the 'take the call' key. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
	Press the OK key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
Call	Press the call key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
# or *	If defined in the phone settings, you can use these keys to initiate the call (*Menu → Features → Key As Send*).

Depending on the system, after dialing the number, the call can be started automatically after a delay without action.

When you are in hands-free mode, you can take the call at any time on the handset by unhooking it.

If your headset has no Off-hook/On-hook key, use the phone keys and switch on the audio on the headset ( ).

To make an external call, dial the outside line access code before dialing your contact number.
The call will start after a timeout of approx. 10 seconds if there is no action taken after dialling.
If you are using multiple SIP accounts on your phone, you can choose which account to use to make the call.

3.2.3 Making a peer to peer SIP call

Your phone is compatible with the peer to peer SIP call. It is able to call phones connected to the same local network. You can call your contact by entering the IP address of your contact's desk phone. Make the call with the headset if connected, or in hands-free mode.

	Open the dialer.
Use one of the following:	
	Press the call key. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
	Press the OK key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
Call	Press the call key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
# or *	If defined in the phone settings, you can use these keys to initiate the call (*Menu → Features → Key As Send*).

The format of the entered IP address must be x.x.x.x or x*x*x*x where x is a decimal value between 0 and 255.

This feature is useful when you have no connection to a communication server (no registration, network problems, etc.). Not all the features are available should this occur and the phone's status should be displayed on the screen. This feature can be deactivated by your administrator.

3.2.4 Calling by name

You can call a contact by his/her name using the search feature in the company directory.
This feature depends on the system configuration. If necessary, contact your administrator.
You can unhook the handset or the headset to make a call with the handset or the headset otherwise you make a call in hands-free mode.

Use the alpha-numeric keyboard key to switch between the numeric and alphabetic keyboard.

	Open the dialer.
abc	Switch to the alphabetical keyboard.
	Enter the first letters of your contact's name. The search runs as soon as you enter a character (predictive search). The matching names are displayed.
	Select the contact to call.
Use one of the following:	
	Press the 'take the call' key. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
	Press the OK key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
Call	Press the call key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
# or *	If defined in the phone settings, you can use these keys to initiate the call (*Menu → Features → Key As Send*).

123

3.2.5 Call from call log

You can call back a contact from the call log.
You can unhook the handset or the headset to make a call with the handset or the headset otherwise you make a call in hands-free mode.

In idle state or from the dialer:	
History	Select this softkey to open call logs from the homepage or the dialer.
	Select the contact to call.
Use one of the following:	
	Press the 'take the call' key. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
	Press the OK key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
Call	Press the call key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
# or *	If defined in the phone settings, you can use these keys to initiate the call (*Menu → Features → Key As Send*).

If you are using multiple SIP accounts on your phone, the call back is made with the SIP account displayed in the call log.

3.2.6 Calling using your personal directory

You can unhook the handset or the headset to make a call with the handset or the headset otherwise you make a call in hands-free mode.

In idle state or from the dialer:	
Directory	Select this softkey to open your local directory from the homepage or the dialer.
	Open a directory (depending on model).
	Select the contact to call.
Use one of the following:	
	Press the 'take the call' key. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
	Press the OK key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
Call	Press the call key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
# or *	If defined in the phone settings, you can use these keys to initiate the call (*Menu → Features → Key As Send*).

If you are using multiple SIP accounts on your phone, you can choose which account to use to make the call.

3.2.7 Calling using speed dial key

You can unhook the handset or the headset to make a call with the handset or the headset otherwise you make a call in hands-free mode.

	Select the key associated with the contact to call.

The SIP account used to make the call depends on the speed-dial key configuration.

3.3 Receiving a call

When receiving a call, you can:

	Lift the handset to take the call.
	Use the headset to take the call. If your headset has no Off-hook/On-hook key, use the phone keys and switch on the audio on the headset ( ).
	Press the loudspeaker/hands-free key to take the call in hands-free mode.
	Press the blinking line key associated with the SIP account receiving the call.
Take call or	Take the call with the headset if connected, or in hands-free mode.
or *Reject call*	Deflect the call to your voicemail.
Silent	Mute the ringer (the call is still incoming but the phone no longer rings).
Deflect	Deflect the call to another contact: Use one of the following: - Using the up and down navigator (if necessary), find the contact to call. - Enter the number or name of the contact to whom the call will be deflected. Deflect the call to the selected contact.

3.4 Switching between audio modes

During the conversation, you can switch between different audio modes (handset, hands-free or headset, if connected) by pressing the loudspeaker/hands-free key until the desired audio mode is displayed: . This feature depends on connected devices. The key is lit when the loudspeaker or hands-free mode is selected.

- You are in conversation with the handset, you can switch between following audio modes by short pressing on the loudspeaker/hands-free key.

- You are in conversation with the headset (headset or headset+loudspeaker), you can switch between following audio modes by short pressing on the loudspeaker/hands-free key.

- You can switch to loudspeaker (group listening mode with handset) when in conversation by pressing the group listening programmable key. First you have to create a group listening programmable key (see chapter: Programmable keys).

For each audio mode, during the conversation, you can adjust the volume by pressing the volume keys. The number of levels depends on the audio mode (8 for handset and headset 10 for hands-free and loudspeaker). The selected volume, for each audio mode, will be saved for future conversations.

- During a conversation.
- Adjust volume by pressing the volume keys.

3.5 Redialing

3.5.1 Call back the last number dialed

	long press: redialing the last number dialed.

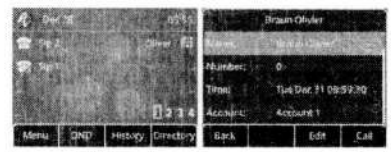
3.5.2 Call back one of the last numbers dialed

	Short press: list of last numbers dialed.
	Select one of the last numbers dialed.
Use one of the following:	
	Press the 'take the call' key. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
	Press the OK key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
Call	Press the call key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.

3.6 Contacts management

3.6.1 Contact card

A contact card can be opened from your local directory.



Directory	Select this softkey to open your directory(-ies).
	Open a directory (depending on model).
	Select a contact.
More → Detail	Open the contact card.
	Use the up-down navigation keys to scroll the page.

The contact card displays information about the contact.

- Avatar: select an avatar for your contact by using right-left navigation keys.
- First name: first name of your contact.
- Last name: last name of your contact.
- Office: office number.
- Mobile: Mobile number.
- Other: Other number.
- Account: If you are using multiple SIP accounts, define which account is used to call this contact.
- Group: Define the group to which this contact belongs in order to make it easier to find.

From this page, you can:

	Modify information about your contact (avatar, name, add new number, etc.). Use the up-down navigation keys to edit a field.

124

3.6.2 Contacts management

Your phone lets you manage contacts in your local directory. With the M7 DeskPhone, you can import contacts from your mobile phone to a specific directory (*External Directory*).

The directory is accessible from the homepage dynamic key or from the menu.

Use one of the following:	
Directory	If configured, use the dynamic key from the home page to access to the directory(-ies) directly.
Menu→ Directory	Select this softkey to open your directory(-ies).

In this user manual, we are using the dynamic key to access directory(-ies).

Directory	Select this softkey to open your directory(-ies). Depending on the model of your phone, your directory is composed of the local directory containing all contacts created on the phone and an external directory containing all imported contacts from your mobile phone (M7).
Local Directory	Open the local directory. Your local directory has displayed all saved contacts and groups. A group contains all contacts belonging to this group (defined in the contact card of the contact).
External Directory	Open the external directory. The external directory is only available on the M7 DeskPhone. Your external directory lists all contacts imported from your mobile phone via Bluetooth®.

From this page, you can:

Search	Search a contact in all directories and groups.
Add	Create a new contact.
Delete	Delete the selected contact.
More	Access more features.
Call	Call the selected contact.
Detail	Open the contact card.
Delete all	Delete all contacts in a directory.
AddGrp	Add a new group.
Enter	List contacts in the selected directory or group.
Back	Return to the main page.

3.6.3 Call your contact

Directory	Select this softkey to open your directory(-ies).
Use one of the following:	
Search	Search a contact in all directories and groups.
	Open a directory (depending on model).

To call your contact:

	Select the contact to call.
First method	
More	Access more features.
Call	Start the call.
Second method	
	Start the call.

If there are several numbers for the same contact, select the desired number.

	Select the desired number.
or *Call*	Start the call.

3.6.4 Create a new contact in your local directory

Directory	Select this softkey to open your directory(-ies).
Local Directory	Open the local directory.
Add	Use the up-down navigation keys to switch from one input field to another.
Switch or	• Avatar: choose a predefined avatar. • Account: if you are using multiple SIP accounts, define which account is used to call this contact. The default SIP account is selected by default. • Group: define the group to which this contact belongs in order to make it easier to find. The group 'All contacts' is selected by default.
<Abc>	• First name: enter first name of your contact. • Last name: enter last name of your contact.
<123>	• Office: enter the office number of your contact. • Mobile: Enter the mobile number of your contact. • Other: Enter another number.
or *Save*	Your contact is added to the directory.

Other method:

- Add a contact from the history.

For external numbers, we recommend you use canonical address formats comprising '+', followed by the country code (e.g. '33') then the number without the first digit. For example, for 0390670000, enter the number +3390670000. To get the '+' sign, long press on the '0' key. This example is for calling a number in France from another country.

3.6.5 Create a new group

Directory	Select this softkey to open your directory(-ies).
Local Directory	Open the local directory.
AddGrp	Use the up-down navigation keys to switch from one input field to another.
<Abc><123>	Enter the name of the group.
or *Save*	Your contact is added to the directory.

3.6.6 Modify a contact

Directory	Select this softkey to open your directory(-ies).
Local Directory	Open the local directory.
	Select the contact to modify.
More	Access more features.
Detail	
	Fill in the contact file. Use up-down navigation keys to edit a field.
or *Save*	To save the contact in the local directory.

3.6.7 Delete a contact in a directory

Directory	Select this softkey to open your directory(-ies).
	Open a directory (depending on model).
	Use the up-down navigation keys to select the contact to delete.
Delete	
or *Ok*	Confirm the deletion.

3.6.8 Delete all contacts in a directory

Directory	Select this softkey to open your directory(-ies).
Local Directory	Open the local directory.
	Use the up-down navigation keys to select a contact.
More	Access more features.
Delete all	
or *Ok*	Confirm the deletion

3.6.9 Delete a group in the local directory

Directory	Select this softkey to open your directory(-ies).
Local Directory	Open the local directory.
Group	Access to all defined group(s).
	Select the group to delete.
Delete	Access to all defined group(s).
or *Ok*	Confirm the deletion.

3.6.10 Delete all group in the local directory

Directory	Select this softkey to open your directory(-ies).
Group	
	Select the group to delete.
Delete all	
or *Ok*	Confirm the deletion.

3.6.11 Import contacts from your mobile phone via Bluetooth® (M7)

To import a contact from your mobile phone you have to pair it to your desk phone.
Before performing the pairing operation, the device must be in detectable mode. Consult the user documentation of your Bluetooth® device.

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Bluetooth	Use up-down and 'ok' navigation keys to select: *Bluetooth*.
Scan	Press the softkey under the following label: *Scan*. Scanning starts. Searching for Bluetooth® equipment. Wait for the detected equipment type and address to be displayed.
Connect	Add the device by pressing on the associated key: *Connect*.
	Enter the PIN code of the device if necessary.

This icon is displayed on your desk phone: .

Depending on your mobile phone, you have to accept to share contacts either during pairing or in connection options. Consult the user manual of your mobile phone.

The contacts are automatically imported into the directory: *External Directory*.

Contacts are kept until another mobile is connected to the M7 or if you delete all imported contacts manually.

125

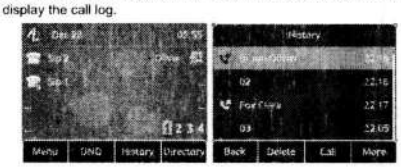
If necessary, you can manually synchronize contacts:

The phone is in idle state.

Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Directory*.
Bluetooth	Use up-down and 'ok' navigation keys to select: *Bluetooth*.
Paired Bluetooth Device	Use up-down and 'ok' navigation keys to select: *Paired Bluetooth Device*. The paired device is listed.
●	Select your connected mobile phone.
More -> Enter > Sync BT Contacts	Use up-down and 'ok' navigation keys to select: *Sync BT Contacts*. Synchronize the contacts.

3.7 Manage the call log (History)

The call log can be consulted and managed when the phone is in the idle state. The main part of the screen is used to display the call log.



The call log (history) is accessible from the homepage dynamic key or from the menu.

Use one of the following:

History	If configured, use the dynamic key from the home page to access to the call log directly.
Menu-> History	Use the menu key to access the call log.

In this user manual, we are using the dynamic key to access the call log.

All call logs associated with the selected contact are displayed with an icon showing the type of call.

	Answered incoming calls.
	Unanswered incoming calls.
	Unanswered incoming call that has been acknowledged.
	Answered outgoing calls.
	Unanswered outgoing calls.

Actions are available from the call log:

Delete	Delete the selected entry. Note that no confirmation is requested.
Call	Call the selected contact.
More	Access more features.
● or *Detail*	Open information about the contact: name, number, time, relevant SIP account, duration.
Delete all	Delete the entire log associated with the selected contact. Note that no confirmation is requested.
Missed	Display missed calls only.
AddCList	Add the contact in your local directory. If the contact already exists, the contact card is edited.
Back	Return to the main page.

3.7.1 Call the contact

History	Select this softkey to open call logs from the homepage or the dialer.
●	Select the contact to call.

Use one of the following:

●	Press the 'take the call' key. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
●	Press the OK key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
Call	Press the call key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.

3.7.2 Display missed calls only

History	Select this softkey to open call logs from the homepage or the dialer.
Missed	Press this key to display missed calls only.

3.7.3 Acknowledge all new missed call logs

All missed calls are acknowledged as soon as you consult the call log (history).

3.7.4 Delete a contact in the call log

History	Select this softkey to open call logs from the homepage or the dialer.
●	Select the contact to delete.
Delete	Delete the selected entry. Note that no confirmation is requested.

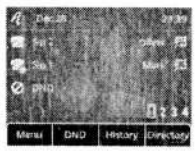
3.7.5 Clear the call log

History	Select this softkey to open call logs from the homepage or the dialer.
More	Access more features.
Delete all	
● or *Ok*	Confirm the deletion.

If you are using multiple SIP accounts on your phone, the concerned SIP account is displayed for each entry of the call log (● or *Detail*).

.8 Speed dial management

Speed dial lets you manage favorite contacts. You can create speed dial keys by programming keys from the homepage.



3.8.1 Create a speed dial key

Use one of the following:

	Long press on a free programmable key.
Menu -> Features -> Programmable Key	Use up-down and 'ok' navigation keys to select: *Programmable Key*.

Create a speed dial key.

Switch or ●	Define the type of programmable key: *Speed dial*.
Account	Associate a SIP account to use to make the call.
<123><Abc>	Enter the number and its label.
● or *Save*	Save the speed dial key.

3.8.2 Make call using speed dial

	Select the key associated with the contact to call.

3.9 Sending DTMF signals

During a conversation you sometimes have to send DTMF signals, such as with a voice server, an automated attendant or a remotely consulted answering machine.

	Enter DTMF code.

To activate or deactivate DTMF mode

The phone is in idle state.

Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Sound	Use up-down and 'ok' navigation keys to select: *Sound*.
DTMF Tone	Use up-down and 'ok' navigation keys to select: *DTMF Tone*.
Switch or ●	To activate or deactivate DTMF mode.
● or *Save*	Validate your choice.
●	To end the settings.

3.10 Mute, so that your contact cannot hear you

You can hear your contact but he/she cannot hear you:

During a conversation.

●	Disable microphone ›› the key lights up.
●	Resume the conversation ›› the key is no longer lit.

3.11 Interphony (auto answer)

In the interphony mode, calls are automatically answered.

Activate the interphony:

The phone is in idle state.

Menu	Press the Menu soft key to access the Main Menu.
Features	Use up-down and 'ok' navigation keys to select: *Features*.
Auto answer	Use up-down and 'ok' navigation keys to select: *Auto answer*.
●	Select the SIP account. All incoming calls to this SIP account will be auto answer.
Switch or ●	Enable the interphony.
● or *Save*	Save the setting.
	This icon is displayed in the status bar.

126

3.12 Make an intercom call

When you make an intercom call, the call is automatically picked-up by your contact, if intercom is enabled on your contact's phone. The ring tone will then be different.

To make an intercom call, you have to create a programmed key: *Intercom*.

- *Account*: select the relevant SIP account.
- *Label*: enter the label of the key, displayed on the home page.
- *Value*: Enter the contact number to call.

3.13 Configure the intercom incoming calls

When you receive an intercom call, the desk phone automatically answers the call if you have authorized the option. You can manage your desk phone behavior when you receive an intercom call.

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Features	Use up-down and 'ok' navigation keys to select: *Features*.
Intercom	Use up-down and 'ok' navigation keys to select: *Intercom*.
Switch or	Select the SIP account. All incoming calls to this SIP account will be auto answer. • *Allow*: enable/disable intercom call. • *Mute*: enable/disable mute. • *Tone*: enable/disable tone. • *Barge*: enable/disable barge.
or *Save*	Save the setting.

3.14 Change PIN code

The PIN code is requested to unlock the phone.
The default PIN code is: 0000.

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Change PIN	Use up-down and 'ok' navigation keys to select: *Change PIN*.
	Enter current PIN code.
	Enter the new PIN code.
	Confirm new PIN code.
or *Save*	Save the setting.
	To end the settings.

3.15 lock / unlock your telephone

Enable the phone lock.

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Phone Lock	Use up-down and 'ok' navigation keys to select: *Phone Lock*.
Switch or	Enable the option: *Lock Enable*.
	To end the settings.

To lock/unlock your desk phone, you have to create a programmed key: *Phone Lock*.

- *Label*: enter the label of the key, displayed on the home page.

3.15.1 Lock your phone

	Select the lock/unlock programmed key.
Ok /	Validate your choice. Your phone is locked. A lock page is displayed.

You can only call emergency numbers, such as 'Operator' or 'Guard', once the phone is locked (max 3 numbers, configured by the administrator).

3.15.2 Unlock your phone

	Unlocking your phone. Your password is required to unlock the phone (the default PIN code is: 0000).

3.15.3 Activate or deactivate the automatic keypad lock

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Phone Lock	Use up-down and 'ok' navigation keys to select: *Phone Lock*.
Switch or	Enable the option: *Auto Lock Enable*.
	Enter the timeout without activity before the keylock (seconds).
or *Save*	Validate your choice.
	To end the settings.

3.16 During conversation

Actions available during conversation:

End	End the call.
Hold	Placing a call on hold.
Transfer	Transfer a call.
Retrieve	Retrieve a call (on hold, parked).
New	Make a second call when the first is on hold.
Swap	Switching between calls.
Conf	Establishing a three-party conference call.
End conf	End the conference with all participants.

3.17 Making a second call during a conversation

During a conversation.	
Hold	Your first call is placed on hold.
New	A dial area and the call log are displayed.
Use one of the following:	
	Enter the number.
→	Select a contact in the call log.
Directory → or *Call*	Call a contact from the local directory.
<abc> → or *Call*	Call your contact using the dial-by-name function.
	Select the 'Redial' function.

3.18 Answering a second call during a conversation

During a conversation, another person is trying to call you. Your are alerted with 3 beeps. The identity of the caller is displayed as long as the call is presented on your phone. The key in front of the SIP account receiving the call is blinking.

Use one of the following:	
	Press the blinking line key associated with the SIP account receiving the call.
Take call or	Take the call with the headset if connected, or in hands-free mode
or *Reject call*	Deflect the call to your voicemail.
Silent	Mute the ringer (the call is still incoming but the phone no longer rings).
Deflect	Deflect the call to another contact: Use one of the following: ○ Using the up and down navigator (if necessary), find the contact to call. ○ Enter the number or name of the contact to whom the call will be deflected. Deflect the call to the selected contact.

As long as the call is presented, you can also choose to deflect the call.

3.19 To cancel your second call and recover the first

You are in conversation with the second contact and the first one is on hold.

Use one of the following:	
	You or the second contact hangs up.
End	Press the softkey under the following label: *End*.
Recover the call on hold:	
Retrieve	Press the softkey under the following label: *Retrieve*. You are on the line with your first contact.

3.20 Placing a call on hold (hold)

During a conversation, you wish to place the call on hold and recover it later, on the same telephone.
Place the call on hold:

Use one of the following:	
	Press the hold key.
Hold	Press the softkey under the following label: *Hold*.

Recover the call on hold:

Use one of the following:	
	Press the hold key.
Retrieve	Press the softkey under the following label: *Retrieve*.
	Press the dedicated account key with call-on-hold icon.

127

3.21 Switching between calls (Broker call)

During a conversation, a second call is on hold.
Use one of the following:

Swap	Press the softkey under the following label: *Swap*.
	Press the hold key.
	Press the dedicated account key with call-on-hold icon.

›› You can talk to the first caller and the second one is on hold.

3.22 Transferring a call

3.22.1 To transfer a call to another contact on hold

During a conversation, a second call is on hold.
Use one of the following:

	Press the transfer key ›› the two callers are connected.
Transfer	Press the softkey under the following label: *Transfer* ›› the two callers are connected.

3.22.2 To transfer your call to another number

During a conversation.
Use one of the following:

	Press the transfer key ›› the first call is on hold.
Transfer	Press the softkey under the following label: *Transfer* ›› the first call is on hold.
New -> or *Call*	Call the recipient of the transfer using the dial a number or dial by name feature or the call log or local directory. Your contact answers.

Use one of the following:

	Press the transfer key ›› the two callers are connected.
Transfer	Press the softkey under the following label: *Transfer* ›› the two callers are connected.

Transfer between two outside calls is not generally possible (depends on country concerned and system configuration).

3.22.3 Blind transfer

You can also transfer your call immediately, without having to wait for your contact to answer.

During a conversation.
Use one of the following:

	Press the transfer key ›› the first call is on hold.
Transfer	Press the softkey under the following label: *Transfer* ›› the first call is on hold.
New -> or *Call*	Call the recipient of the transfer using the dial a number or dial by name feature or the call log or local directory.
B transf	Before your contact answers the call, select *B transf* ›› the two callers are connected.

Transfer between two outside calls is not generally possible (depends on country concerned and system configuration).

3.23 Three-way conference

During a conversation, a second call is on hold.
Use one of the following:

	Press the conference key ›› you are in conference mode.
Conf	Press the softkey under the following label: *Conf* ›› you are in conference mode.

3.23.1 End the conference with all participants

You are in conference mode.
Use one of the following:

	Press the on-hook key ›› the conference is ended.
End conf	Press the softkey under the following label: *End conf* ›› the conference is ended.

3.23.2 After the conference, to leave your two contacts talking together

You are in conference mode.
Use one of the following:

	Press the transfer key ›› the two participants remain on the call together.
Transfer	Press the softkey under the following label: *Transfer* ›› the two participants remain on the call together.

3.24 Talk simultaneously to more than 2 contacts (five-way conference with internal contacts) (M7, M5)

This feature is available only for the following device: M7 DeskPhone, M5 DeskPhone.

You are in three-way conference call.
Use one of the following:

	Press the hold key.
Hold	Press the softkey under the following label: *Hold*.
New -> or *Call*	Call a new participant by using the dial a number or dial by name feature or the call log or local directory. You are in conversation with the new participant.
Join	The new participant is joining the conference call.

When the maximum of participants is reached, you will not be able to make a new call to add a new participant.

3.24.1 End the conference with all participants

You are in conference mode.
Use one of the following:

	Press the on-hook key ›› the conference is ended.
End conf	Press the softkey under the following label: *End conf* ›› the conference is ended.

If you are a participant (you did not initiate the conference call), you can exit the conference by pressing the on-hook key.

3.25 Hide your phone number

you can choose to hide your identity when calling.

	The phone is in idle state.
Menu	Press the Menu soft key to access the Main Menu.
Features	Use up-down and 'ok' navigation keys to select: *Features*.
Anonymous	Use up-down and 'ok' navigation keys to select: *Anonymous*.
	Select the SIP account whose phone number will be hidden.
Switch or	Enable the option: *Anonymous*.
or *Save*	Validate your choice.
	To end the settings.

›› your identity will be hidden.

3.26 Reject anonymous calls

The phone is in idle state.

Menu	Press the Menu soft key to access the Main Menu.
Features	Use up-down and 'ok' navigation keys to select: *Features*.
Anonymous rejection	Use up-down and 'ok' navigation keys to select: *Anonymous rejection*.
	Select the SIP account to reject anonymous calls.
Switch or	Enable the option: *Anonymous rejection*.
or *Save*	Validate your choice.
	To end the settings.

3.27 Do not disturb

You can make your terminal temporarily unavailable for all calls.

The phone is in idle state.

Menu	Press the Menu soft key to access the Main Menu.
Features	Use up-down and 'ok' navigation keys to select: *Features*.
DND	Use up-down and 'ok' navigation keys to select: *DND*.
Switch or	Enable the option: *DND*.
or *Save*	Validate your choice.
	To end the settings.

To deactivate the Do not disturb feature, follow the same procedure.

To have a direct access to this feature, program a key on the home page (see chapter: Programmable keys).

From the Web Management, it is possible to enable/disable the feature for all accounts declared on the phone (the administrator password of the phone is requested).

129

3.28 Forwarding to a number

When you are absent or already in communication (all lines are busy), all your calls are forwarded to the defined number. You can define a programmed key to activate forward.

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Features	Use up-down and 'ok' navigation keys to select: *Features*.
Call Forward	Use up-down and 'ok' navigation keys to select: *Call Forward*.
Select the type of call forwarding required	
Always Forward	All your calls are immediately forwarded to another number.
Busy Forward	All your calls are forwarded to another number when you are already on the line.
No Answer Forward	All your calls are forwarded to another number when you cannot answer.

Switch or	Activate the forward.
Forward To	Enter the destination number.
or *Save*	Validate your choice.
	To end the settings.

To have a direct access to this feature, program a key on the home page (see chapter: Programmable keys).

We recommend using programmed key on the home page to find the status of the phone easily. If a feature is activated, the corresponding key is lights up.

From the Web Management, it is possible to enable/disable the feature for all accounts declared on the phone (the administrator password of the phone is requested).

3.29 Cancelling all forwards

If you are using a programmed key, just press it.

he phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Features	Use up-down and 'ok' navigation keys to select: *Features*.
Call Forward	Use up-down and 'ok' navigation keys to select: *Call Forward*.
Select the type of call forwarding to cancel.	
Always Forward	All your calls are immediately forwarded to another number.
Busy Forward	All your calls are forwarded to another number when you are already on the line.
No Answer Ferward	All your calls are forwarded to another number when you cannot answer.

Switch or	Deactivate forward.
or *Save*	Validate your choice.
	To end the settings.

3.30 Listen to your voicemail

This feature depends on the system configuration. If necessary, contact your administrator.

The message key flashes when you have received a new voicemail or if you have missed calls.

	Press the messaging key. Number of messages received is displayed.
X new voice message(s)	Use up-down and 'ok' navigation keys to access voicemail.
	The number of new messages is displayed for each registered account. Select the relevant account.
or *Enter*	Call your voicemail. Follow the instructions from the voicemail server.

You can use the menu to access voicemail: *Menu* → *Voicemail* → *View Voicemail*.

3.31 Defining a 'hotline' number

If configured, the 'hotline' number is dialed immediately or after a time delay when you take the line by picking up the handset, by pressing the hands-free button or pressing the call button of the headset. To configure the 'hotline' number:

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Features	Use up-down and 'ok' navigation keys to select: *Features*.
Hotline	Use up-down and 'ok' navigation keys to select: *Hotline*.
Number	enter the number of the 'hotline'.
Delay	Enter the time delay in seconds before the 'hotline' number is dialed, if no action is performed during this time (0 – 10s). The 'hotline' number is immediately dialed if the delay time is set to 0s.
Switch or	Enable the feature.
or *Save*	Validate your choice.
	To end the settings.

Follow the same procedure to deactivate the feature.

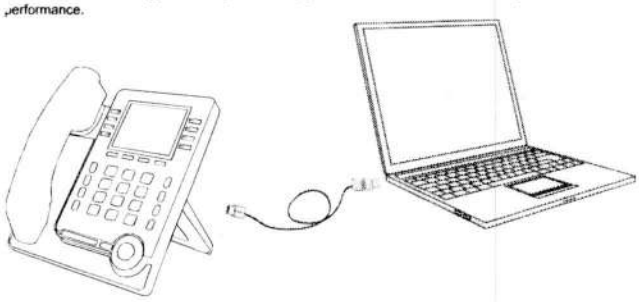
This feature can be configured via the Web Management.

4 Do more with your desk phone

Your desk phone is designed to evolve with its environment. It can do more than just establish communication between people or keep in touch with your contacts, your enterprise.
This chapter describes some use-cases with your phone.

4.1 Use your desk phone as a USB audiohub for your computer

Your phone can be used as an external audio playback/recording device for your personal computer (PC). Use the hands-free mode of your desk phone with applications such as Rainbow, OpenTouch conversation for PC, Skype, etc. Or you can simply listen to music with an outstanding audio performance.



4.1.1 Installation

4.1.1.1 Prerequisites

Before using your DeskPhone as a USB audiohub for your computer, make sure your computer meets the minimum hardware and software requirements.

The lists below are for information only and are not contractual. Contact your administrator if necessary.

- The supported operating systems are:

Windows	Mac OS X	Linux
7 (32-bit or 64 bit) 8 (32-bit or 64 bit) 8.1 (32-bit or 64 bit) 10 (32-bit or 64 bit)	10.9 (Maverick) 10.10 (Yosemite) 10.11 (El Capitan) 10.12 (Sierra), 10.13 (High Sierra), 10.14 (Mojave), 10.15 (Catalina)	Compatible with most Linux distributions.

- USB connector: we recommend a USB 3.0 port (USB 2.0 or 1.0 port can reduce performance).
- We recommend using the latest version of audio applications or web browser.

4.1.1.2 Connect your computer to your desk phone

You can use a USB-A or USB-C connectors of the DeskPhone to connect the PC. A stand-alone USB cable is not provided with your set.

- Configure your desk phone to use it as an audiohub.

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Usb	Use up-down and 'ok' navigation keys to select: *Usb*.
	Select the USB port you are using to connect the PC (USB-A, USB-C).
Switch or	Select the mode: *Slave*.
or *Save*	Validate your choice.
	To end the settings.

- Create the programmable key: *Audio Hub* (see chapter: Programmable keys).
  The programmable key allows you to control the audio on the phone (pause, play).
  As long as the PC is not connected, the following icon is displayed in front of the programmable key and on the status bar:
- Connect your computer to the USB-A or USB-C connector of your desk phone with the USB cable (not provided). The phone is recognized as a sound device on computer (for example 'Echo cancelling speakerphone' with Windows). The following icon is displayed in front of the programmable key and on the status bar:

4.1.1.3 Set the default audio device for Windows

In most cases, your desk phone is ready to be used when connected to your computer. However, it is sometimes necessary to manually configure the playback and recording default device. The configuration depends on the operating system of the connected computer. Consult the user manual of the operating system of your computer.

4.1.1.3.1 Windows

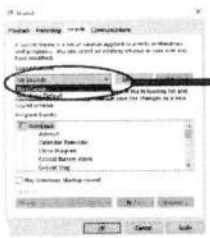
- Open the sound control panel from the Windows configuration panel or the sound icon in the Windows notification area.

129

- In the 'Playback' tab: Select your desk phone as the default device.

- In the 'Recording' tab: select your desk phone as the default device, if you are using the hands-free mode of your desk phone with communication applications such as Rainbow, OpenTouch Conversation for PC, for example.

- Activating/Deactivating the sounds



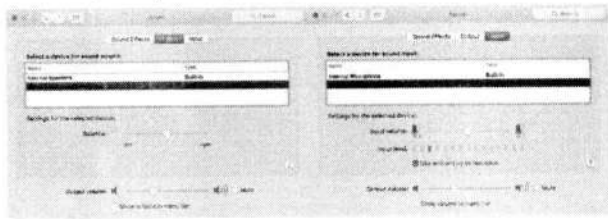
If you set your desk phone as the default audio device, all of the sounds from your computer are played on your desk phone, like notifications.

1. Activating/Deactivating the sounds.
2. Apply.

Consult the user manual of the operating system of your computer.

4.1.1.3.2 Mac OS 10.9 and above

- Open System Preferences -> Sound.
- Select your desk phone in output and input tabs:



4.1.2 Using your phone as an audio hub

When audio starts playing on the PC, it will also be played on the phone.

The audio hub programmable key lets you control the playback:

	The audio is playing on the phone. Pause the audio by pressing the programmable key.
	Play/resume the audio by pressing the programmable key.

The volume can be adjusted on the phone by using volume keys or via the PC.

You can use the hands-free mode of your desk phone with communication applications such as Rainbow, OpenTouch Conversation for PC, for example.

The audio is paused when you receive an incoming call or perform any other operation on the phone that is not related to the audio hub. You can resume the audio at any time by pressing the audio hub programmable key.

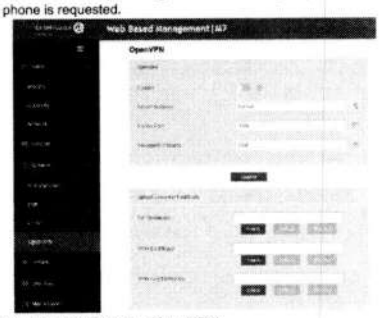
4.2 Configure your phone for remote working

Your IP phone is compatible with remote working (VPN) via a secure connection (encrypted). A Virtual Private Network (VPN) is a technology that allows a device to create a tunneling connection to a server and becomes part of the enterprise's network (VPN server's network). VPN tunnels are secured with OpenVPN protocol with TLS authentication, credentials and certificates.
To establish an VPN connection, make sure you have information about connection from the hosting provider:

- Connection settings: server address, port and protocol.
- CA root certification file (.crt).
- Client certification file (.crt).
- Client key file (.key).

The VPN connection must be configured, started and stopped from the Web Management device.

- Open the Web Management device.
  When the phone is connected to the network, your administrator can access the Web Management via a web browser by entering the IP address of your phone. The administrator password of the phone is requested.



- In the settings tab, select the VPN menu (OpenVPN).
- Enter the required information (VPN server address, port and protocol).
- Upload security files: choose a file and select the upload button for each file (CA root certification, Client certification, Client key file).
- Enable VPN.
- Apply.
- The desk phone restarts.

The connection will be established every time the system reboots until you disable the VPN manually.
To disable the VPN:

- Open the Web Management device.
- In the settings tab, select the VPN menu (OpenVPN).
- Disable the VPN.
- Enable VPN.
- Apply.
- The desk phone restarts.

4.3 Connect your phone to the Wi-Fi

It is possible to connect your DeskPhone to the wireless network of your company or at your home, in case of remote worker (VPN). You have to plug a Wi-Fi dongle into the USB-A connector of your phone: To know the supported dongle, please refer to the Alcatel-Lucent Enterprise website or contact your administrator. The dongle can use 2.4Ghz and 5Ghz bands, but we recommend using a 5Ghz Wi-Fi network to ensure the best audio quality. The best radio signal will be automatically selected. A specific icon is displayed in the status bar when you are connected to a Wi-Fi access point: .

4.3.1 Configure the wireless network

You can manually configure your DeskPhone to connect to the selected Wi-Fi access point (SSID). This section is useful when you connect your phone to your personal Wi-Fi network for teleworking or to check the Wi-Fi configuration of the phone. Before configuring your phone, you need to know the name and the network security key (passphrases) of the Wi-Fi access point.

Plug the Wi-Fi dongle into the USB-A connector of the DeskPhone.
Start your desk phone (powered by PoE or adapter).

The phone is in idle state.

Menu	Press the Menu soft key to access the Main Menu.
Advanced Setting	Use up-down and 'ok' navigation keys to select: *Advanced Setting*. The administrator password of the phone is requested. Enter the administrator password. Validate.
Wi-Fi	All scanned SSIDs are listed according to signal strength (it may take a few seconds to display the available networks). Use the up-down navigation key to scroll the page. : this icon, displayed at left of the SSID name, represents the signal strength: the more waves, the better the signal. During connection establishment, this icon is displayed at right of the SSID name. : this icon indicates the current connected SSIDs. : this icon indicates SSIDs already saved in the phone.
or *Detail*	Display all information about the corresponding wireless network, such as the SSID, encryption mode, channel, signal strength.
Connect	Connect the phone to the selected wireless network.
	If the wireless network is not already saved, enter the network security key (passphrase) if requested.Use the alpha-numeric keyboard key to switch between the numeric and alphabetic keyboard. : during connection establishment, the Wi-Fi icon is displayed (1 to 4 waves).
	If the connection is successful, a pop-up is displayed on your phone. A specific icon is displayed in the status bar when you are connected to a Wi-Fi access point: . The SSID and authentication is automatically saved, if it has not already been saved.

To switch back to the wired network, unplug the Wi-Fi dongle, connect the Ethernet cable and restart the desk phone.

130

4.3.2 Manage wireless network

The Wi-Fi manager allows you manage all saved wireless network configurations on your phone. If the wireless network is available and saved on your phone, the connection is automatic. If there are several networks available, the best signal will be used.

4.3.2.1 Open the Wi-Fi manager

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Advanced Setting	Use up-down and 'ok' navigation keys to select: *Advanced Setting*. The administrator password of the phone is requested. Enter the administrator password. Validate.
Wi-Fi → Wi-Fi Manager	Use up-down and 'ok' navigation keys to select: *Wi-Fi Manager*.

4.3.2.2 Add a new wireless network

Open the Wi-Fi manager.	
Add	Depending on the Wi-Fi network, enter the SSID, security mode, encryption mode and password of the wireless network. Use the alpha-numeric keyboard key to switch between the numeric and alphabetic keyboard.
Save	Save the wireless network.

4.3.2.3 Modify a saved wireless network

Open the Wi-Fi manager.	
	Use up-down navigation keys to select the saved wireless network to edit.
or *Edit*	Depending on the Wi-Fi network, enter the SSID, security mode, encryption mode and password of the wireless network. Use the alpha-numeric keyboard key to switch between the numeric and alphabetic keyboard.
Save	Save the wireless network.

4.3.2.4 Remove a saved wireless network

pen the Wi-Fi manager.	
	Use up-down navigation keys to select the saved wireless network to delete.
Delete	Delete the selected wireless network.

4.4 Desk sharing

The availability of this feature depends on your system and its configuration. Please contact your administrator before using these services.

This feature allows you to use any compatible SIP DeskPhone in your company with your own phone number. When you activate your account on a desk phone, you retrieve your entire phone configuration: local directory, history (depending on the system configuration). After reboot the phone restarts with its initial configuration.

We recommend activating only one phone number at a time to ensure that all incoming calls are received on the same phone.

This feature has to be activated by the administrator of the phone.

Before using this feature, you have to program a key on the home page with the following feature: *Hot Desking*.

- *Label*: enter the label of the key, displayed on the home page.

4.4.1 Login to desk sharing

When you start the desk sharing feature, all user configurations on the phone are cleared.

	Select the desk sharing programmed key.
Ok	Validate to ensure all current user configurations will be cleared.
	Enter the phone number and password of the SIP account.
or *Save*	Confirm. The desk phone is loading the Sip account configuration. You can use it as your own desk phone.

4.4.2 Logout of desk sharing

When you want to leave the office and retrieve the initial state of the phone, you have to reboot the phone.

4.5 Third-Party Call Control (3PCC) with Rainbow application

This feature depends on the system configuration. If necessary, contact your administrator.

Your phone is compatible with third-party call control to manage calls (basic features) from your computer via the Alcatel-Lucent Rainbow application:

- Make and answer calls.
- Put your contact on hold or retrieve.
- Transfer a call.
- Consultation and configuration of the mail box (if defined).

Please consult the Rainbow support site for more information: https://support.openrainbow.com/hc/.

5 Programming your telephone

5.1 Adjusting the audio functions

These features can be configured via the Web Management.

5.1.1 Select the melody

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Sound	Use up-down and 'ok' navigation keys to select: *Sound*.
Ringing	Use up-down and 'ok' navigation keys to select: *Ringing*.
Ext. Melody/Int. Melody	The melody must be chosen for external and internal calls: *Ext. Melody/Int. Melody* (optional).
	Select the melody of your choice (16 tunes).
or *Enter*	Validate your choice.
	To end the settings.

5.1.2 Adjusting the ringer volume

The phone is in idle state.	
	Select the volume you want (10 levels).

5.1.3 Configure the ringtone

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Sound	Use up-down and 'ok' navigation keys to select: *Sound*.
Ringing	Use up-down and 'ok' navigation keys to select: *Ringing*.
Ring mode	Use up-down and 'ok' navigation keys to select: *Ring mode*.
Switch or	• *Normal ringing* A normal ring signals an incoming call. • *Progressive ringing* A progressive ring signals an incoming call.
Switch or	Enable or disable the silent mode: *Silent mode*. The phone no longer rings. The LED flashes to signal an incoming call.
or *Save*	Validate your choice.
	To end the settings.

5.1.4 Configuring discreet mode (beep)

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Sound	Use up-down and 'ok' navigation keys to select: *Sound*.
Ringing	Use up-down and 'ok' navigation keys to select: *Ringing*.
Beep	Use up-down and 'ok' navigation keys to select: *Beep*.
Switch or	• *0 Beep* A normal ring signals an incoming call. • *1 Beep* A beep followed by the ring signals an incoming call. • *3 Beep* Three beeps followed by the ring signals an incoming call.
or *Save*	Validate your choice.
	To end the settings.

5.1.5 Seat mode

Your desk phone supports the seat mode. The seat mode lets your administrator switch the ringing onto the loudspeaker, the headset or both. This feature is configurable from the Web Management. Contact your administrator for more information.

5.2 Selecting language

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Language	Use up-down and 'ok' navigation keys to select: *Language*.
	Select the language of your choice.
or *Save*	Validate your choice.
	To end the settings.

5.3 Adjusting the brightness of the desk phone

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Display	Use up-down and 'ok' navigation keys to select: *Display*.
Backlight	Use up-down and 'ok' navigation keys to select: *Backlight*.
Use right-left navigation keys to adjust the brightness.	
Active Level	Adjust the brightness when the phone is in use.

131

Inactive Level	Adjust the dimmed brightness when the phone is not in use.
Backlight Time	Set the time-out duration for the phone backlight.
	Select the language of your choice.
or *Save*	Validate your choice.
	To end the settings.

5.4 Enable screensaver and define the delay

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Display	Use up-down and 'ok' navigation keys to select: *Display*.
Screen saver	Use up-down and 'ok' navigation keys to select: *Screen saver*.
Use right-left navigation keys to adjust the brightness.	
Screen saver	Enable screensaver and define the delay (use right-left navigation keys).
Wait Time	Enter the idle time in seconds before the screensaver starts.
or *Save*	Validate your choice.
	To end the settings.

5.5 Define the voicemail number

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Voicemail	Use up-down and 'ok' navigation keys to select: *Voicemail*.
Set Voicemail Number	Use up-down and 'ok' navigation keys to select: *Set Voicemail Number*.
	Enter the voicemail number of the corresponding account.
or *Save*	Validate your choice.
	To end the settings.

5.6 Programmable keys

Depending on the phone, you can program between 15 and 27 keys. You can connect an add-on module to have more programmed keys (sold separately).

5.6.1 Create a programmable key

	Long press on a programmable key.
Switch or	Define the type of programmable key. Depending on the type of key, fill in the options.
or *Save*	Save the programmed key.

5.6.2 Delete a key

	Long press on a programmed key.
Switch or	*Undefined*
or *Save*	Save.

5.6.3 Type of programmed key

- *Undefined*: delete a programmed key.
- *Account*: line Key.
  - *Account*: select the relevant SIP account.
  - *Label*: enter the label of the key, displayed on the home page.
- *Speed Dial*: speed dial key (direct call key).
  - *Account*: select the relevant SIP account.
  - *Label*: enter the label of the key, displayed on the home page.
- *BLF* (Busy Lamp Field): indicates whether another extension connected to the same system is busy or not. Use the BLF key to make a direct call or pick up a call from the defined number.
  - *Account*: select the relevant SIP account.
  - *Label*: enter the label of the key, displayed on the home page.
  - *Value*: the number of the extension which the user wishes to monitor.
  - *Extension*: a list of extensions which the user wishes to monitor.
- *BLF List*: a list of extensions which the user wishes to monitor. The list is defined by your administrator via the WBM or a configuration file.
  - *Label*: enter the label of the key, displayed on the home page.
- *Hold*: place or retrieve the call on hold.
  - *Label*: enter the label of the key, displayed on the home page.
- *Transfer*: transfer function.
  - *Label*: enter the label of the key, displayed on the home page.
- *Conference*: conference call function.
  - *Label*: enter the label of the key, displayed on the home page.
- *ReCall*: redial the last incoming number.
  - *Label*: enter the label of the key, displayed on the home page.
- *DND*: do not disturb function.
  - *Label*: enter the label of the key, displayed on the home page.

- *Directory*: open the local directory.
  - *Label*: enter the label of the key, displayed on the home page.
- Forward: immediate forward to a number.
  - *Label*: enter the label of the key, displayed on the home page.
  - Value: dial the destination number.
- *Voicemail*: consulting your voice mailbox.
  - *Account*: select the relevant SIP account.
  - *Label*: enter the label of the key, displayed on the home page.
  - *Value*: enter the voicemail prefix code.
- *Hot Desking*: desk sharing function.
  - *Label*: enter the label of the key, displayed on the home page.
- *Prefix*: open the dialpad with predefined prefix.
  - *Account*: select the relevant SIP account.
  - *Label*: enter the label of the key, displayed on the home page.
  - *Value*: Prefix.
- *DTMF*: sending a predefined DTMF signal during conversation.
  - *Label*: enter the label of the key, displayed on the home page.
  - *Value*: DTMF code.
- *DirectPickup*: call pick-up.
  - *Account*: select the relevant SIP account.
  - *Label*: enter the label of the key, displayed on the home page.
  - *Value*: enter the pickup code followed by the extension number.
- *GrpPickup*: group call pick up.
  - *Account*: select the relevant SIP account.
  - *Label*: enter the label of the key, displayed on the home page.
  - *Value*: enter the group pickup code followed by the group number.
- *Headset*: activate/Deactivate Headset mode.
  - *Label*: enter the label of the key, displayed on the home page.
- *GroupListen*: activate/deactivate group listen audio mode.
  - *Label*: enter the label of the key, displayed on the home page.
- *Intercom*: make a call to a contact who will answer the call automatically.
  - *Account*: select the relevant SIP account.
  - *Label*: enter the label of the key, displayed on the home page.
  - *Value*: enter the contact number to call.
- *Audio Hub*: use your desk phone as a USB audiohub for your computer.
  - *Label*: enter the label of the key, displayed on the home page.
- *XML Browser*: display an XML page.
  - *Label*: enter the label of the key, displayed on the home page.
  - *Value*: enter the URL of the XML page.
- *Phone Lock*: lock/unlock the phone.
  - *Label*: enter the label of the key, displayed on the home page.

These keys can be also configured by the administrator via Web Management or via the configuration file.

Led behavior may differ depending on the system configuration.

For more information, contact your installer or administrator.

5.7 Call pick-up

You hear a telephone ringing in an office where no-one can answer. If authorised, you can answer the call on your own telephone.

The system can be configured to prevent call pick-up on some telephones.

Before using this feature, you have to program a key on the home page with the following feature: *GrpPickup*, *DirectPickup*.

- If the telephone ringing is in your own pick-up group:
  select the programmed key: *GrpPickup*.
- If the telephone ringing is not in your pick-up group:
  select the programmed key: *DirectPickup*.

5.8 Install a USB accessory (Headset, Handsfree, Loudspeaker)

- Connect the accessory to the USB connector.
- When you plug the accessory in the USB port, the USB accessory is automatically detected. If an another accessory is already connected with the same function (USB and jack), a pop-up will ask you to select your preferred accessory to use for this function.

If you are using an external hands-free device, configure the audio for this purpose:

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Sound	Use up-down and 'ok' navigation keys to select: *Sound*.
External Device	Use up-down and 'ok' navigation keys to select: *External Device*.
Switch or	Enable external hands-free.
or *Save*	Validate your choice.

If you want the headset to ring only when receiving an incoming call, you must activate the headset mode.

5.9 Headset mode

You can use a headset with your phone. If you want the headset to ring only when receiving an incoming call, you must activate the headset mode.

Before using this feature, you have to program a key on the home page with the following feature: *Headset*.

The phone is in idle state. **Connect the headset to the desk phone.**	
	Select the programmed key: *Headset*. This icon is displayed on your desk phone:

132

5.10 Define time and date format

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Time and Date	Use up-down and 'ok' navigation keys to select: *Time and Date*.
Switch or	*Date*: choose the date format.
Switch or	*Time*: select Time Format.
or *Save*	Validate your choice.
	To end the settings.

5.11 Manage Bluetooth® device (M7)

This feature is only available with compatible Bluetooth® desk phone. Otherwise the corresponding menu is not displayed or is inactive. You can pair one Bluetooth® device, such as headphones, with your desk phone.

5.11.1 Installing a Bluetooth® device

Before performing the pairing operation, the device must be in detectable mode. Consult the user documentation of your Bluetooth® device.

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Bluetooth	Use up-down and 'ok' navigation keys to select: *Bluetooth*.
Scan	Press the softkey under the following label: *Scan*. Scanning starts. Searching for Bluetooth® equipment. Wait for the detected equipment type and address to be displayed.
Connect	Add the device by pressing on the associated key: *Connect*.
	Enter the PIN code of the device if necessary.

This icon is displayed on your desk phone: .

If you are using an external hands-free device, configure the audio for this purpose:

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Sound	Use up-down and 'ok' navigation keys to select: *Sound*.
External Device	Use up-down and 'ok' navigation keys to select: *External Device*.
Switch or	Enable external hands-free.
or *Save*	Validate your choice.

5.11.2 List connected devices

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Bluetooth	Use up-down and 'ok' navigation keys to select: *Bluetooth*.
Paired Bluetooth Device	Use up-down and 'ok' navigation keys to select: *Paired Bluetooth Device*. The paired devices are listed.
	Select a device.
or *More*→*Detail*	Display information about the selected device (name, MAC address).

5.11.3 Removing a Bluetooth® accessory (headset, handset, etc.)

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Bluetooth	Use up-down and 'ok' navigation keys to select: *Bluetooth*.
Paired Bluetooth Device	Use up-down and 'ok' navigation keys to select: *Paired Bluetooth Device*. The paired devices are listed.
	Select a device.
Delete	Remove the selected device.

5.11.4 Removing all Bluetooth® accessories

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Directory*.
Bluetooth	Use up-down and 'ok' navigation keys to select: *Bluetooth*.
Paired Bluetooth Device	Use up-down and 'ok' navigation keys to select: *Paired Bluetooth Device*. The paired device is listed.
More→*Delete all*	Remove all devices. Note that no confirmation is requested.

5.11.5 Edit the name of your desk phone

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Bluetooth	Use up-down and 'ok' navigation keys to select: *Bluetooth*.
Edit My Device Info	Use up-down and 'ok' navigation keys to select: *Edit My Device Info*. The name and the MAC address of your desk phone is displayed. You can change the name.
or *Save*	Validate your choice.

6 Contacting your administrator (technical support)

If necessary you may need to contact your administrator.
Before contacting your administrator, make sure you have information such as your phone's codes and software version to hand.

6.1 Technical code / Date code

The codes are located under the backshell of the phone. This label is an example and does not represent the one placed on your phone.

1. Technical code.
2. Date code.

6.2 Software version / Display network settings (IP address)

The software version can be viewed on the phone by following this path:

The phone is in idle state. Use one of the following:	
Menu→*Status*	

133

6.3 Access to administrator configuration

6.3.1 Administrator settings menu

The phone is in idle state.	
Menu	Press the Menu soft key to access the Main Menu.
Advanced Setting	Use up-down and 'ok' navigation keys to select: *Advanced Setting*.
<Abc><123>	Enter the administrator password.
	This section allows the administrator to set IP parmeters, certificates, LDAP servers, DM URL (for configuration files), and SIP Accounts. The administrator can also restore factory settings. The DM URL is used to automatically download the phone's configuration file, including all parameters, when the phone switches on.

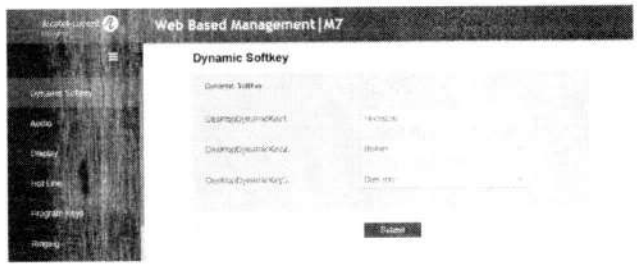
6.3.2 Web Management (WM)

Web Management offers the administrator an easy way to configure the settings of your phone through a web page hosted by your phone.

When the phone is connected to the network, your administrator can access the Web Management via a web browser by entering the IP address of your phone. The administrator password of the phone is requested. When connecting for the first time, the default password has to be modified.

From the Web Management, your administrator can configure all SIP accounts of the desk phone.

The administrator can define the 3 dynamic keys displayed on the homepage.



All configuration parameters of the desk phone can be managed from the Web Management.

- Audio (Ringing, Tone, hearing aids...).
- Backlight, Screensaver, automatic lock.
- Date format, time format.
- Forward, Do not disturb.
- Hotline number.
- Intercom.
- Programmed keys displayed on the desk phone.
- USB mode (host, slave).
- Network configuration (DM, DNS, Ethernet, IP parameters, LDAP).
- VPN configuration.

7 Accessories

The ALE-supported accessories are intended to work smoothly on most/all of our clients (hardphones, softphones). The list of accessories presented in this document is not contractually binding and may be modified without prior warning.

7.1 List of accessories

7.1.1 USB headset

You can use a USB headset to handle calls on the DeskPhone M3 / M5 / M7. To know the supported eadsets, please refer to the Alcatel-Lucent Enterprise website or contact your administrator. Unlisted JSB headsets may not work properly if you connect them to your phone. For more information on using your USB headset, refer to the corresponding documentation from the manufacturer.

7.1.2 Add-on module

- M20 Expansion Module.
- EM200 Smart Expansion Module.

7.1.3 Conference module

- Konftel EGO.
- 8135s IP Conference Phone.

7.1.4 Adapter

- USB C to USB-A CABLE (box of 10).

7.1.5 USB Dongle

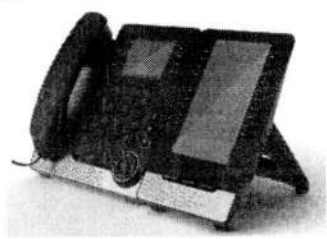
To know the supported dongle, please refer to the Alcatel-Lucent Enterprise website or contact your administrator.

7.1.6 Other accessories (headsets)

Please consult the following sites of providers for compatible headsets:

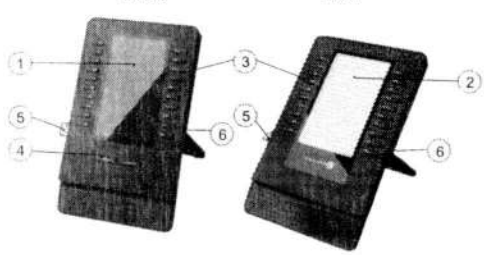
- https://www.plantronics.com/us/en/solutions/alcatel-lucent
- https://en-de.sennheiser.com/alcatel-lucent-headsets-unified-communications
- https://www.emea.jabra.com/business/for-your-platform/alcatel-lucent

7.2 Add-on module



Phone capabilities can be extended with Add-ons:

- The EM200 add-on offers 60 additional keys with LED, color screen.
- The EM20 add-on offers 20 additional keys with LED and paper label.

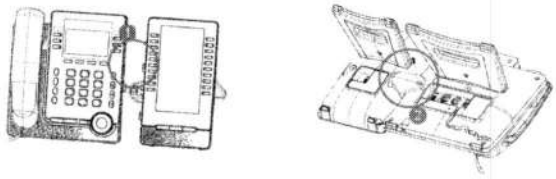


1	LCD screen.	4	Page navigation keys.
2	Paper label.	5	Connector to connect the device to the desk phone or already connected add-on (USB-A).
3	Programmable keys.	6	Universal Serial Bus (USB-a) connector. This connector is used for: • Connect a USB headset. • Connect an add-on module. • Connect a Wi-Fi dongle*.

*To know the supported dongle, please refer to the Alcatel-Lucent Enterprise website or contact your administrator.

134

7.2.1 Install the add-on to the desk phone



1- Insert the add-on USB-A connector into the USB-A socket of the desk phone.
2- Use the add-on support to fix it to the desk phone using the provided screw.
3- The add-on is powered by the desk phone if the desk phone is connected to an external power adapter.
If your desk phone is powered via PoE, we recommend connecting the EM200 to an USB-C power adapter (DC 5V/2A output, not provided with the add-on).
4- Restart the desk phone (unplug and plug in the power jack if you are using an external power adapter or the Ethernet connector – LAN).

7.2.2 Install more than one add-on module

It is possible to connect up to three similar add-on modules. It is not possible to connect EM20 and EM200 add-ons together.

Depending on how the desk phone is powered, you need to use an external power adapter (DC 5V/2A output, not provided with the add-on) connected to the add-on.

Your desk phone is powered via PoE:

- You can connect up to two EM20 without an external power adapter.
- You can connect three EM20s. One of the add-ons must be connected to an external power adapter.
- You can connect up to two EM200s. One of the add-ons must be connected to an external power adapter.

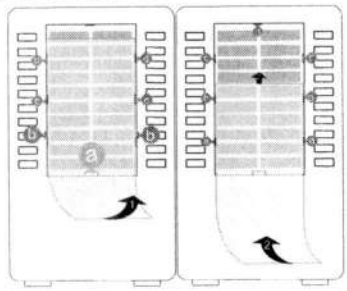
Your deskphone is powered via an external power adapter:

- You can connect up to three EM20s without an external power adapter.
- You can connect up to two EM200s without an external power adapter.
- You can connect three EM200s. One of the add-ons must be connected to an external power adapter.

To attach another add-on, affix and connect the new add-on to the one that is already connected:

- The first add-on is connected to the desk phone.
- Insert the new add-on USB-A connector into the USB socket of the installed add-on.
- Use the add-on support to fix it to the add-on using the screw provided.
- Restart the desk phone (unplug and plug in the power jack if you are using an external power adapter or the Ethernet connector – LAN).

7.2.3 Changing or updating the paper label



- Remove the protective cover (1): insert a thin object (or your fingernail) in the slot (a) to lift the protective cover. Slide the cover down. The cover is held in place by small notches, take care not to break the plastic cover near the notches.
Remove the cover from the other notches (c, d) by moving the cover gently from right to left.
- Remove the paper label with a thin object.
- Replace the paper label and protective cover (2):
the cover or the paper can only be placed in the right way. Insert the paper label under the first notches (a). Then, insert the other notches by sliding the paper up (b, c, d). If necessary, you can gently press the paper near the notch to help it to slide under the notch.
- Put the protective cover back in the same way.

Paper label and paper label cover can be ordered separately.

7.3 Konftel EGO

The Konftel EGO is a compact and portable conference module. It provides OmniSound® audio technology for very high-quality HD audio conversations. In addition, the Konftel EGO comes with a 1000m Ah Li-ion battery for up to 12 hours of meetings and calls. The Konftel EGO can be connected to your desk phone, mobile phone, tablet and computer. This section describes how to use the conference module with your desk phone. To use the Konftel EGO with your computer, mobile phone, or tablet, or for more information about the device, see the complete user manual of the device (8AL90358xxAA).

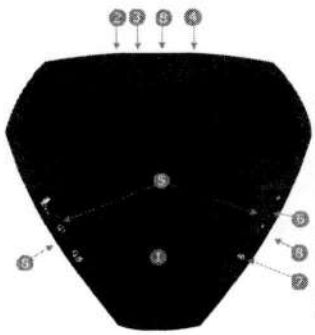
7.3.1 Box content

- Konftel EGO

- Konftel EGO case

- Micro-USB cable

7.3.2 Description



1 Color display.

2 Off/on button.
- Push the button to start.
- Hold down the button for five seconds to manually switch off.
- The Konftel EGO switches off automatically after 30 minutes.

3 USB connector (micro type B).

4 3.5 mm, 4 pole jack (TRRS standards: CTIA)

5 Audio control buttons
- Activating and disactivating the mute.
- Turn up the volume.
- Turn down the volume.
- Start/pause music.
- Previous music.
- Next music.

6 Call control buttons
- End the call.
- Answer the call.

7 Button for pairing Bluetooth®.

8 IED (IEDs on all sides).

7.3.3 LED description

- Steady yellow: the device is switched on.
- Blue steady: connected through Bluetooth®.
- Green steady: microphone is enabled/call in progress (Bluetooth®).
- Flashing green: incoming call (Bluetooth®).
- Flashing blue: pairing or connecting in progress (Bluetooth®).
- Red steady: microphone switched off during calls (mute).
- Flashing red: Low battery.
- Flashing slowly: the call is placed on hold (Bluetooth®).

7.3.4 Icons displayed on the screen

The icons are normally displayed for a couple of seconds on connection. The same symbol is displayed in red when the connection is broken.

	USB device connected.		Incoming call or call in progress via Bluetooth®.
	Incoming call or call in progress via USB.		Music mode via Bluetooth®.
	Music mode via USB.		Headset connected.
	Visible for pairing via Bluetooth®.		Volume adjustment (number of bars indicates the volume selected).
	Reconnecting to Bluetooth® device.		Microphone switched off (mute).
	Bluetooth® device connected.		Battery status.

7.3.5 Battery charge

Displayed automatically when there is 1 hour remaining and then every 5 minutes. The number of bars in the battery icon indicates the charging status. The battery needs charging when the icon turns red. Charging the battery with a USB cable.

7.3.6 Turning off and on

The Konftel EGO starts automatically when it is connected with the provided USB cable to the desk phone or powered-up computer.

- Push the button to start the device manually.
- Hold down the button for five seconds to manually switch off.

7.3.7 Connect the device to the desk phone using the USB cable

- Connect the device to the USB type A connector of the desk phone using the provided USB cable. The Konftel EGO automatically starts. The following icon is displayed on the screen of the device:
- The Konftel EGO is detected as a hands-free device. Select 'Konftel Ego' on the pop-up displayed on your desk phone.
- The device is ready for use.

135

7.3.8 Connect the device to the desk phone using Bluetooth® (compatible Bluetooth® desk phone)

- Switch on the Konftel EGO.
- Put the device in detectable mode: hold the Bluetooth® button down for two seconds on the Konftel EGO: . The following icon is displayed on the screen of the device: .
- From your desk phone, pairing the Konftel EGO:

	The phone is in idle state.
Menu	Press the Menu soft key to access the Main Menu.
Basic Setting	Use up-down and 'ok' navigation keys to select: *Basic Setting*.
Bluetooth	Use up-down and 'ok' navigation keys to select: *Bluetooth*.
Paired Bluetooth Device	Use up-down and 'ok' navigation keys to select: *Paired Bluetooth Device*.
Scan	Press the softkey under the following label: *Scan*. Scanning starts. Select the relevant equipment: "Konftel Ego"
Connect	Add the device by pressing on the associated key: *Connect*.

- The Konftel EGO is successfully paired. The following icon is displayed a couple of seconds on the Konftel EGO screen: . It is detected as a Bluetooth® headset. The following icons are displayed on the status bar of your desk phone: ,

P86_9182: .

To remove the device, follow instructions described in the section: "Removing a Bluetooth® accessory (headset, handset, etc.)".

7.3.9 Using the Konftel EGO

The Konftel EGO is used as an external hands-free device.

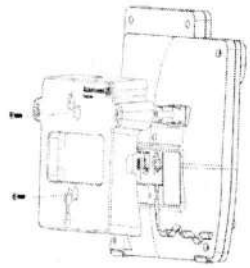
- When you receive a call, the device is ringing and an icon is displayed on the screen: / . The leds are flashing green.
- ✓ Answer the call.
- Activate/deactivate the mute feature during a conversation. The mute icon is displayed on the Konftel EGO if activated:
- Use the volume buttons of the desk phone or Konftel EGO to turn the volume up or down.
- ✕ End the call. You can end the call from the desk phone.

You can resume the call with the handset at any time by unhooking it or by switching between audio mode ( ).

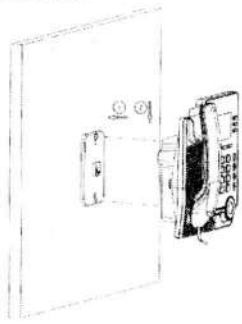
7.4 Wall mounting kit

To mount your phone on the wall, you need to install a standard wall plate that you can easily find on the market. Follow the manufacturer's instructions to install the wall plate on the wall. When the wall plate is fixed, you can prepare your phone and mount it on the wall. The wall mount kit is sold separately (refer to the following chapter for the reference: Ordering information).

1. Fix the support with the phone by using the 2 screws provided (the size of screw is M3x8mm).



2. Hang the assembled phone with wall mounted kit on the wall plate.



7.5 Developer and Solution Partner Program (DSPP)

The mission of the DSPP is to support a broad ecosystem of developers and partners throughout the desk phone lifecycle. In this context, certification tests are performed between partner applications or devices and Alcatel-Lucent Enterprise's platforms. It certifies proper inter-working with partner applications or devices. Results of certification tests for headsets can be consulted by following the links below.

- IWR-0121: Sennheiser Headsets / Desk phones
  https://www.al-enterprise.com/-/media/assets/internet/documents/sennheiser-headsets-terminals-iwr-0121-ed10-en.pdf
- IWR-0018: Jabra Headsets for hardphones
  https://www.al-enterprise.com/-/media/assets/internet/documents/iwr-0018-ed03-gn-jabra-headsets-amplifiers-omnipcxplatformsterminals.pdf
- IWR-0164: Plantronics-Headsets-Amplifiers
  https://www.al-enterprise.com/-/media/assets/internet/documents/plantronics-headsets-amplifiers-iwr-0164-ed04.pdf

8 Technical specifications

	M7	M5	M3
Width	207 mm (8, 2 in)	207 mm (8, 2 in)	207 mm (8,15 in)
Height	183 mm (7,2 in)	183 mm (7,2 in)	183 mm (7,2 in)
Weight	810 g (1,79 lbs)	800 g (1,77 lbs)	806 g (1,78 lbs)
2-degree adjustable foot	40° - 55°	40° - 55°	40° - 55°
Color	Gray	Gray	Gray
Display	3.5 inch color, 320 x 240 pixels	2.8 inch color, 320 x 240 pixels	2.8 inch monochrome with backlight, 128 x 64 pixels
Memory (Flash/SDRAM)	256 MB/256MB	256 MB/256MB	256 MB/128MB
Power over Ethernet (IEEE 802.3af)	Class 2	Class 2	Class 2
Power consumption (PoE) Idle – Active(w/o Add-on, w/o USB)	< 3.5 W	< 3.5 W	< 3.5 W
Operating conditions	-5°C - +45°C (23°F - 113°F)	-5°C - +45°C (23°F - 113°F)	-5°C - +45°C (23°F - 113°F)

	Konftel EGO
Maximum distance between the phone set and the device	
Width	145 mm (5,7in)
Depth on a table	135 mm (5,31in)
Height	32 mm (1,26in)
Weight	230 g (0,51 lb.)
Adjustable foot stand range	
Color	Licorice black
Power consumption	Battery: 1000 mAh Li-ion aC adapter: power and charging via USB.
UL/CSA Ratings	
Operating conditions	5° C à 40° C (41 °F - 104 °F)

136

9 Ordering information

M7 DeskPhone	3MK27003AA
M5 DeskPhone	3MK27002AA
M3 DeskPhone	3MK27001AA
EM20 Expansion Module (add-on module)	3MK27006AA
EM200 Smart Expansion Module (add-on module)	3MK27007AA
USB C to USB-A cable (box of 10)	3MG08020AA
Wide Band Comfort Handset	3MG27032AA
USB Binaural Headset	3GV28057AB
Wall mounting kit	3MK27008AA
USB-C Power Adapter (100–240 V AC/5 V DC) (US)	3MK08005US
USB-C Power Adapter (100–240 V AC/5 V DC) (EU)	3MK08005EU
USB-C Power Adapter (100–240 V AC/5 V DC) (RW)	3MK08005RW
Konftel EGO	3MG08017AA
8135s IP Conference Phone	3MG07040AA

10 Guarantee and clauses

Current Safety and Regulatory Statements relate to the following products (do not apply to accessories): M3 DeskPhone, M5 DeskPhone, M7 DeskPhone.

10.1 Safety Instructions

- Changes or modifications to the equipment not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- Magnets could affect the functioning of pacemakers and implanted heart defibrillators. Keep a safe distance between your pacemaker or implant defibrillator and the handset which includes magnetic elements: 4 centimeters (1,6 inches) at least.
- To limit the risk of interference, people with pacemakers must keep the wireless telephone away from their equipment (minimum distance of 15 cm/6 inches).
- It is recommended to follow the standard acceptance procedures before using this equipment in human safety critical areas (hospitals...).
- The handset includes magnetic elements that may attract sharp metallic objects. To prevent injury, before each use ensure sharp metallic objects are not stuck to the earpiece and microphone.
- Avoid using phones (other than cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use this device in environments where there is a danger of explosion.
- Do not plug this phone into an Integrated Services Digital Network (ISDN) connection or into a regular Public Switched Telephone Network (PSTN) connection. This can result in severe damage to the phone.
- Never allow your telephone to come into contact with water.
- To clean your telephone, use a soft damp cloth. Never use solvents (trichlorethylene, acetone, etc.) which may damage the plastic parts of your telephone. Do not use aerosol cleaners.
- M3/M5/M7 DeskPhone: this product is intended to be supplied, either via the Ethernet (LAN) port (Minimum Class 2 according to IEEE802.3af), or via the DC-in by a Certified Direct Plug-In Power Unit approved as 'LPS' (Limited Power Source) against IEC/EN/UL/CSA 62368-1 and rated 5V dc, minimum 2A. Allowed power supply is: WB-10N05 – Asian Power Devices Inc.
- EM200/EM20 Expansion Module: this product is intended to be powered either via the USB-A port from the M3/M5/M7 DeskPhone, or via the USB-C DC-IN by a Certified Direct Plug-In Power Unit approved as an 'LPS' (Limited Power Source) in accordance with IEC/EN/UL/CSA 62368-1 and rated 5V DC, minimum 2A. Other power supply products from the same family are permitted: WB-10N05 – Asian Power Devices Inc.
- If you are connected to a POE connection do not use an external Power Supply.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected cables must all be completely indoors.
- The M7 DeskPhone offers a Bluetooth® radio interface for Bluetooth® devices with a frequency range of 2402-2480 MHz, radiated power 5 mW.

10.2 Regulatory Statements

EUROPE

This equipment complies with the essential requirements of following directives: 2014/53/EU (RED), 2014/30/EU (EMC), 2014/35/EU (LVD), 2009/125/EC (ErP), 2011/65/EU (RoHS), 2015/863 (EU). Declaration of Conformity may be obtained from: ALE International 32 avenue Kléber – 92700 Colombes, France - ebg_global_supportcenter@al-enterprise.com

USA and Canada

Phones with Bluetooth® comply with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

'hone has been tested without Bluetooth® and was found to comply with the limits for a class B digital levice, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance wit the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try correcting the interference by consulting the dealer.

This product meets the applicable Industry Canada technical specifications and the applicable Innovation, Science and Economic Development Canada technical specifications.

Exposure to Radio Frequency Signals

This equipement complies with radiation exposure limits set by FCC/IC and the Council of European Union for an uncontrolled environment. This equipment has very low levels of RF energy and is deemed to be compliant without testing of the specific absorption rate (SAR).

User Instructions

Use this product in temperatures between -5°C to +45°C (23°F to 113°F).
This product is intended for use in an indoor environment only. This apparatus is Hearing Aid Compatible (HAC).

Acoustic shock protection

Maximum sound pressure level for handset is compliant with European, US and Australian standards.

Directive 2003/10/EC specifying the risks inherent in noise at work

The ring contributes towards overall daily noise - at its maximum setting, the level is 105 dBA at 60 cm from terminal. To reduce the level, the following is recommended:- reduce the setting (9 levels of 5 dB) - program a progressive ring.

Privacy

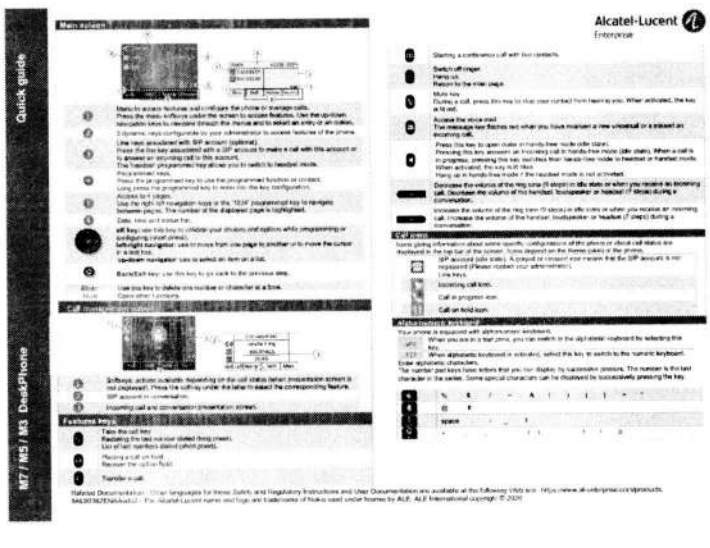
Privacy of communications may not be ensured when using any Bluetooth® device.

Disposal

The equipment must be returned to a collection point for electronic equipment waste disposal.

Related Documentation

Other languages for these Safety and Regulatory Instructions and User Documentation are available at the following Web site: https://www.al-enterprise.com/products.



137

Contacts management	
[illegible]	Select this softkey to open contacts management.
[illegible]	Create a new contact.
[illegible]	Delete the selected contact.
[illegible]	Access more features.
[illegible]	Call the selected contact.
[illegible]	Open the contact card.
[illegible]	Delete all contacts in the local directory.
[illegible]	Add a new group.
[illegible]	List all contacts in the selected group.
[illegible]	Return to the main page.

Contact card	
[illegible]	Select this softkey to open contacts management.
[illegible]	Open the contact card. Modify a contact.
[illegible]	Return to the main page.

[illegible]	
[illegible]	Access the call log.
[illegible]	Delete the selected entry. Note that no confirmation is requested.
[illegible]	Call the selected contact.
[illegible]	Access more features.
[illegible]	Open information about the contact: name, number, time, relevant SIP account, duration.
[illegible]	Delete the entire log associated with the selected contact. Note that no confirmation is requested.
[illegible]	Display missed calls only.
[illegible]	Add the contact in your local directory. If the contact already exists, the contact card is edited.
[illegible]	Return to the main page.

Making a call	
[illegible]	Select the SIP account to use to make the call. A dial area and the list of last number dialed are displayed.
[illegible]	Dial the number.
[illegible]	Calling by name.
[illegible]	Call from call log.
[illegible]	Calling using your personal directory.
Use one of the following:	
[illegible]	Press the 'take the call' key. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
[illegible]	Press the OK key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
[illegible]	Press the call key to start the call. Make the call with the active device: handset if unhooked, headset if connected, otherwise in hands-free mode.
# or *	If defined in the phone settings, you can use these keys to initiate the call ([illegible] → [illegible] → [illegible]).

Receiving a call	
[illegible]	Lift the handset to take the call.
[illegible]	Use the headset to take the call. If your headset has no Off-hook/On-hook key, use the phone keys and switch on the audio on the headset.
[illegible]	Press the loudspeaker/hands-free key to take the call in hands-free mode.
[illegible]	Press the blinking line key associated with the SIP account receiving the call.
[illegible]	Take the call with the headset if connected, or in hands-free mode.
[illegible]	Deflect the call to your voicemail.
[illegible]	Deflect the call to another contact.

During conversation	
[illegible]	End the call.
[illegible]	Placing a call on hold.
[illegible]	Transfer a call.
[illegible]	Retrieve a call (on hold, parked).
[illegible]	Making a second call during a conversation.
[illegible]	Switching between calls.
[illegible]	Establishing a three-party conference call.
[illegible]	End the conference with all participants.
[illegible]	Mute/unmute the selected participant.

Settings	
[illegible]	Press the softkey settings.
[illegible]	Select the melody. Adjusting the ringer volume. Configure the ringtone. Configuring discreet mode (beep).
[illegible]	To activate or deactivate DTMF mode.
[illegible]	Adjusting the ringer volume.
[illegible]	Selecting language.
[illegible]	Adjust the brightness when the phone is in use. Adjust the dimmed brightness when the phone is not in use. Set the delay before the screensaver starts.
[illegible]	Display IP and MAC addresses and software version.
[illegible]	Access phone features: Call Forward, DND, Auto Answer, Programmable key, Anonymous, Key As Send, Hotline, Default Account, Intercom.
[illegible]	Define voicemail number. Access to registered SIP account voicemail.
[illegible]	Manage Bluetooth® device (M7).

Technical specifications

Mechanics

- Weight: 1486 g (3.27 lbs) including handset
- Depth: 167 mm (6.57 in)
- Width: 252 mm (9.92 in)
- Height: 204 mm (8.03 in)
- Color: Black
- Adjustable foot stand ranging from 25° to 60°
- Ingress protection (IP): 22

Display

- Seven-inch screen graphical TFTLCD color touch screen display
- Wide video graphics array (WVGA): 800x480, 16:9 format
- External display through HDMI: Up to 1280 x 720
- Capacitive touch screen technology
- Ambient light sensor
- LCD backlight:
  - Manual adjustment based on user- defined level
  - Auto-brightness mode based on ambient light and user-defined level

Connectivity

- LAN: 10/100/1000 Ethernet
- PC through 10/100/1000 integrated Ethernet switch
- Universal 3.5 mm audio and stereo jack, 4 pins, following the
- Cellular Telephone Industries Association (CTIA) / American Headset Jack (AHJ) standard
- Two USB ports (1.1/2.0) to connect external camera, audio equipment, low smartphone charging or USB stick
- RJ9 connector for corded handset (optional)
- Bluetooth embedded: Headset, earphones, handset, loudspeaker and hands-free support
- HDMI 1.4a output, support for screen replication and dedicated HD video display

Power

- 802.3AF Power over Ethernet (PoE)
- Class 3 support

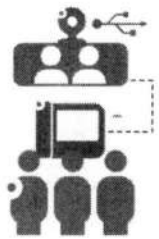
Audio

- HD audio:
  - Wideband loudspeaker
  - Wideband Bluetooth handset
  - Wideband, comfort and wired handset
- Full-duplex speakerphone
- Acoustic echo cancellation
- Automatic Gain Control (AGC) to adjust audio volume and comfortwhile in conference

Video

- H264 Baseline Profile Level 3.0
- Picture-In-Picture (self-preview overlay)
- Power line flicker compensation
- Hot-plug/unplug for an external USB camera
- HD video display through an HDMI output
- Internal HD camera:
  - 720p at 25 fps
  - 5 MP
- Mechanical shutter for privacy HDMI

Figure 1. Video Conferencing configuration



Keys and navigation

- Sensitive keys with a contextual LED management:
  - Mute
  - Volume +/Volume -
  - Audio mode selection: Handsfree, loudspeaker, headset, or handset
  - Hang-up
  - Communication services: active communications, call history, voice mail access, and message waiting indicator
  - Dial pad / keypad
  - User services and settings: Video self- view, routing, overflow, and advanced telephony subscription (including lock, supervision, and CLIR)
  - Home key for immediate access to home page and menus
- Touch screen navigation
- Gestures to activate most frequently used functions such as dial-by-name, video controls, HDMI output, and programmable keys

Alcatel-Lucent 8088 Smart Deskphone

The 8088 Smart DeskPhone delivers instant video collaboration to executives, managers and information workers.

This elegant and exclusive phone offers a 7" large touch screen for video display and an intuitive experience. Any small huddle room becomes a video conferencing room helped to the embedded camera and the wideband audio.

The 8088 has also a Bluetooth handset and a Bluetooth headset pairing, for wireless mobility up to 10 meters from your desk.

Its Android platform provides to anyone the capability to deploy customized and secured app. With the Alcatel-Lucent Rainbow collaboration app, see at a glance who's available and transform, through one tap, any call into an instant video conference with colleagues connected to Rainbow from any device.

Features	Benefits
Alcatel-Lucent Rainbow collaboration app	See at a glance who's connected, easy as one tap to call colleagues connected to Rainbow from any device.
Video conferencing	Transform any huddle room into a video conferencing room, with the 7" Touch screen and embedded HD camera
Support Android apps	Deploy customized and secured app to all users
Wideband Audio quality	Enjoy high audio quality for better comfort
Bluetooth connectivity	Connect a Bluetooth handset or a Bluetooth headset, for wireless mobility up to 10 meters from your desk

Products supported

- Alcatel-Lucent OpenTouch® Multimedia Services, OpenTouch Business Edition, (from Release 2.1 including OmniVista 8770 Network Management System)
- OXO Connect and OXO Connect Evolution from release 3.0 and higher
- As of OmniPCX Enterprise 12.1, offers the full range of telephony services found in Alcatel-Lucent acclaimed communication servers -- unsurpassed in terms of functionality, features, reliability and quality of service

Please refer to 8088 User Manual for more information regarding available features and restrictions.

User-based customization

- Audio file player (MP3, WAV)
- Image and photo viewer (JPG, BMP, PNG)
- Access to local settings for:
  - Screensaver or user-defined
  - Ring tone and notification melodies (more than 10 choices)
  - Background image or user defined
  - Colored skins
  - Audio equipment management
  - User preferences (such as home page and backlight)

Accessories in the catalog

- Wideband comfort handset, corded
- Bluetooth handset
- PoE injector
- 48 V power adapter
- Headsets (for and up-to-date list, see the catalog)

Third-party application support

Dedicated business applications can be deployed on the 8088 Smart DeskPhone.

Centralized management

- Dynamic Host Configuration Protocol (DHCP)/ Automatic VLAN Assignment (AVA)
- Link Layer Discovery Protocol for Media Endpoint Devices (LLDPMED) (802.3 AB)
  - Extensions: VLAN assignment, PoE management, inventory, geolocation
  - HTTP/ HTTPS
- Software upgrade
  - Fast upgrade mode: Software downloads in the background. The device is available to the user during audio and video calls as well.
  - ~1 min of device unavailability during boot time
  - Scheduling through Alcatel-Lucent OmniVista® 8770 Network Management System
- Device configuration based on company standards: Power management and telephony service configuration, such as speakerphone, Bluetooth, automatic lock, audio accessory availability, audio management, and security
- Customizable user interface (skin, melody, colors and background image) using Smart-Custo for DeskPhone, graphical application to build new skin on the 8088 Smart DeskPhone.
- Centralized date and time management (Simple Network Time Protocol, SNTP)

Quality of Service

- 802.1 p/Q
- Differentiated services code point (DSCP)

Security

- HTTPS for secure HTTP access
- 802.1x Message Digest 5 (MD5)/TLS: Customer certificate management (with centralized deployment) for authentication
- Denial of service (DoS) attack protection: Flooding
- Session Initiation Protocol (SIP) message authentication through IP filtering
- Address Resolution Protocol (ARP) spoofing protection
- Transport Layer Security (TLS) 1.2 standard
- Secure Hash Algorithm (SHA)-2 support
- Audio SIP TLS and Secure Realtime Transport Protocol (SRTP) encryption

Internationalization and localization

- Support for 29 languages and input method editors, such as Pinyin, Katakana, Hiragana, and Hangul

Accessibility

- Hearing aid compatible (HAC)
- Incoming call blinking LED: Back and front visibility

Communication services

- Telephony services: Call, answer, deflect, enquiry, hold, broker, transfer and conference controls
- Multi-line management
- Call log: Missed, outgoing and incoming calls
- Dual-tone multi-frequency (DTMF)

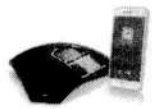
Business communication services

- Place, answer and manage wideband voice, HD video and conferences
- Business caller ID and picture presentation
- On-call services: Deflect, add participants, remove participants, DTMF
- Universal directory access
  - Place an audio or video session with a single tap
  - Add contacts to a unified favorites list across devices
  - View the picture, real-time telephony presence and availability of favorite contacts
- Single identity across devices
  - Select user defined routing rules
  - Route to one or several devices
  - Rapid session shift
  - Supervision screening and call pick-up
  - Manager-assistant screening
  - View and manage a unified call and messaging history across devices
  - Consult and manage a unified visual voicemail across devices
- Lock and unlock
- SIP survivability:
  - Automatic fallback on Alcatel-Lucent OmniPCX® Enterprise Communication Server (CS) or on OmniPCX Enterprise Passive Communication Server (PCS)
  - Automatic fallback on thirdparty server (AAPP) - No reboot required

Contact management

- Add, edit and delete local contacts
- Favorites list management, centralized with other devices

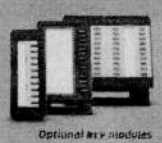
Alcatel·Lucent Enterprise

	8088 BT	8078s BT	8068s BT	8058s (IP)	8028s (IP)	8018 (IP)	8008G	8135s
	Smart DeskPhone	*Premium DeskPhone*	*Premium DeskPhone*	*Premium DeskPhone*	*Premium DeskPhone*	*DeskPhone*	*DeskPhone*	*IP Conference Phone*
Visit our Comparison Tool								
Additional models	8088 8088 & 8088 BT No Cam	8078s	8068s	8039s (Digital)	8029s (Digital)	8019s (Digital)	8008 (100 Mbit/s) 8008G CE, 8008 CE (SIP)	
Usage	Executives Huddle rooms	Executives Managers Huddle rooms	Managers Knowledge workers Attendants Hot-desking	Managers Knowledge workers Attendants Hot-desking	Information workers Hot desking	Information workers Hot desking Lobby Hotel rooms	Information workers Hot desking Lobby Corridors	Meeting room (up to 70 m2)
Differentiating experience	Video collaboration Android Apps 7" touch color screen Touch navigation Bluetooth handset (BT)	5" touch color screen Touch navigation Bluetooth handset (BT) Alphabetic keyboard Optional key modules	3.5" color screen 10 contextual keys Bluetooth handset (BT) Alphabetic keyboard Optional key modules	3.5" color screen (IP) 10 contextual keys USB headset port (IP) Alphabetic keyboard Optional key modules	Backlit screen 6 contextual keys 4 programmable keys USB headset port (IP) Alphabetic keyboard Optional key modules	Compact format Backlit screen 6 contextual keys 4 programmable keys USB headset port (IP)	Compact format Backlit screen (G) 6 contextual keys Directory lookup key Gigabit Eth. PC port (G)	Control by mobile app OmniSound quality Expansion microphones 5-way audio bridge
Superwideband audio[G]		■	■	■ (IP)				
Protocol	ALE or SIP	Dual ALE/SIP	Dual ALE/SIP	Dual ALE/SIP	Dual ALE/SIP	Dual ALE/SIP	Dual ALE/SIP, SIP (CE)	SIP

DELIVER SUPERIOR CUSTOMER EXPERIENCES WITH ALCATEL-LUCENT ENTERPRISE PHONES

Connection™ to Alcatel-Lucent Rainbow
One number mobility · Video collaboration · AI integrations

Wireless mobility
Bluetooth handset
- Pairing with Bluetooth headset or smartphone



Optional key modules

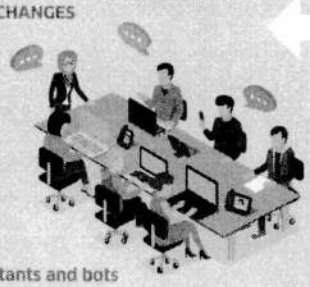
Instant connection
Alphabetic keyboard
- Super-fast search and call
- Optional key modules: 10 keys, 14 keys, 40 keys

Expert communications
Access to all phone system services from the screen
- 10 contextual keys with LED
- Welcome, screening, queuing, team features provided out-of-the-box
- Unified call history from any device

Quality conversations
Superwideband[G] audio
- Wideband audio on all phones
- USB headset port
- 3.5 mm headset jack

ELEGANT, STYLISH DESIGN. YOUR PHONES BECOME YOUR BRAND ADVOCATES!

BUSINESS COMMUNICATIONS FACE NEW DRIVER OF CHANGES



35%

Digital assistants and bots
By 2023, 35% of workers will start working with bots or other forms of AI (IDC)

75%

Mobile workplace
More than 75% of workers would be more loyal to their organization if it offered flexible work options (FlexJobs).

Video collaboration
Business phones connected to a collaboration solution will help people work together wherever they are.

MAKE A DIFFERENCE: CHOOSE CLOUD-ENABLED BUSINESS PHONES

The Alcatel-Lucent Enterprise business phones connect to the Alcatel-Lucent Rainbow cloud, and to AI-enabled applications, right from your desk.

Make life easier
for your teams and provide your customers with a quality communication experience that leverages AI-enabled applications and cloud-based video collaboration.

86%

Customer experience
By 2020, 86% of buyers will pay more for a better customer experience (Walker Study).

Quality communications
With super-wideband audio, all communications will come across loud and clear.

Alcatel-Lucent Business Phones: Deliver a Superior Customer Experience

In this age of digital transformation, your customers expect **quality interaction, impeccable service,** and **fast response** from your teams.

Over **40 million** workers offer their customers **a superior experience** with Alcatel-Lucent Enterprise phones. **Join them!**

ALE Business Phones

Alcatel·Lucent Enterprise

Alcatel·Lucent Enterprise

Alcatel·Lucent Enterprise

Economical and reliable on-site mobility solutions

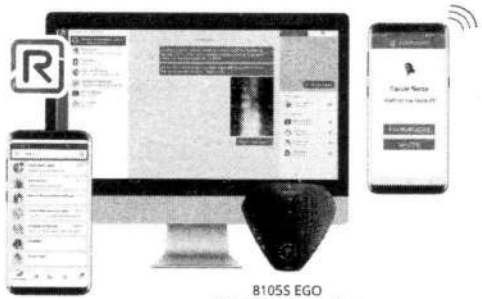
- Discover our new VoWLAN 8158s/8168s handsets, compatible with 802.11 a/b/g/n radio networks and 802.11.r quality of service and roaming standards
- Discover our complete DECT offer featuring:
  - ¬ Standard DECT (IBS/RBS) and IP DECT (8378 DECT IP-xBS) bases for indoor and outdoor use, adaptable to any connection (TDM or IP) and any size of building and site
  - ¬ A large range of DECT handsets. Discover the models best suited to the healthcare sector:
    - The compact, robust, antibacterial DECT 8254 Handset with red emergency button
    - The **DECT 8244** Handset with red emergency button, using Bluetooth® technology for precise localisation
    - The **DECT 8262** Hardened Handset with IWP* function associated with Bluetooth Low Energy technology

8158s/8168s

The ✪ of 8378 DECT IP-xBS terminal

- High-density base station (11 channels) with dedicated channels for alarming
- Superior scalability for campuses, such as university hospitals
- Transparent air update service of DECT Handsets binary code
- Can be combined with standard Alcatel-Lucent TDM DECT base station including roaming and handover services

8254 8244 8262



8105S EGO
Portable conferencing module

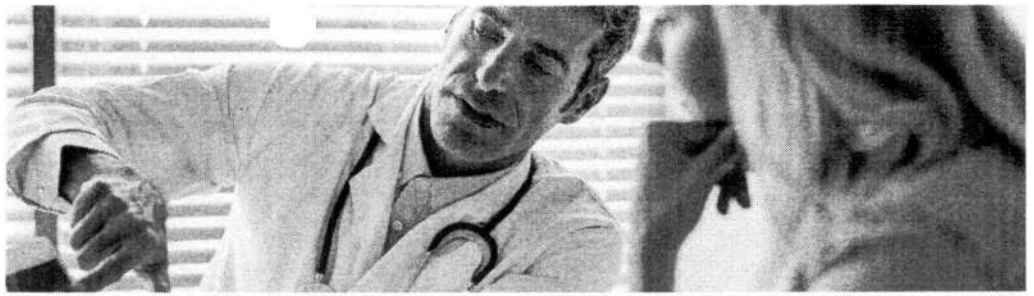
The ✪ of Rainbow

- Customisable cloud collaboration solution including a free subscription
- Protected data **: GDPR, ISO 27001, and French HDS certification
- Compatible with PRO SANTE CONNECT (French national health identity provider)
- Hybrid model: Connect OXE to the cloud service to control your office terminal and/or call any OXE user or external user from your Rainbow client
- Rainbow options: Rainbow Alert and Rainbow Room
- Off-the-shelf connectors ***: CRM, UC (Microsoft® Teams), LMS with Rainbow Classroom, Third-party PBX, and more
- API for integrating connectivity into business application

Address mobility and collaboration needs

- Adapt your working environment to meet current requirements for remote working, mobile telephony, and multi-site team needs
- Use communications and collaboration services to work as a team: For example, easily make a "one-click" call with your desktop phone while sharing your PC screen to improve understanding and help with decision-making
- Arrange instant video conferences using the Web or a smartphone and set up multi-disciplinary consultative meetings with fellow clinicians
- Using the presence functions, quickly identify who is available to answer your questions (for example, who is not on the phone or in a meeting)
- Share files: The cloud provides access to all types of documents such as a care sheet, a simple prescription, or large DICOM format images
- Maintain social links by chatting with your colleagues on your smartphone, wherever they are
- Add video capabilities to a meeting room optimising time to connect with one-click video meetings (Rainbow Room)
- Generate persistent alert message with text or photo and allow the recipient(s) to acknowledge or ignore the emergency notification using Rainbow Alert

* IWP: Isolated Worker Protection detects fall, shock, immobility, among others.
** GDPR: General Data Protection Regulation & HDS: Health Data Hosting
*** CRM: Customer Relationship Management, UC: Unified Communications, LMS: Learning Managing System, PBX: Private Branch Exchange



Alcatel-Lucent Enterprise, communication and collaboration solutions leader in healthcare

Alcatel-Lucent Enterprise is a recognised healthcare facilities and emergency services partner in France and around the world.

We are present in many hospitals and university hospitals as well as fire, rescue, and emergency services. This success is the result of ALE systems' reliable, wide-ranging features and security, as well as our technological know-how.

Our goal is to contribute to the healthcare facilities' digital transformation by offering proven communications and network infrastructure technologies.

We connect patients, healthcare professionals and stakeholders within their ecosystem to optimise the care pathway.

To succeed with this digital transformation we have developed an ecosystem of partnerships (For example: the Developer and Solution Partners Program, Major Benefactor of the largest French hospital cluster, among others) and innovated through participation in technology and solution events (such as: Hacking Health Camp and Call for Expression of Interest for the hospital of the future).

What is digital transformation?

Digital transformation uses technology to improve the patient experience, make life easier for healthcare staff, facilitate the secure exchange of data, and speed up decision-making processes.

Alcatel-Lucent OmniPCX® Enterprise Purple (OXE Purple)

The heart of your efficient and robust real-time communications system for the digital age

OXE Purple is a proven communication server based on a software-only platform that handles multimedia calls from Alcatel-Lucent and third-party vendor phones, including TDM, IP, and SIP.

OXE Purple provides the building blocks for any IP and/or TDM communications solution by integrating the very latest Linux, XML, SIP and VXML technologies, and QSIG, CSTA and SIP open standards. Superior scalability allows OXE Purple to support from 10 to 100,000 users spread over several geographic sites.

It also offers extremely reliable, real-time, carrier-grade performances with unrivalled, 99.999% availability.

In addition, it supports a wide variety of apps and telephones:

- Access your messages from an internal or external telephone using a centralised voice messaging solution, such as **Alcatel-Lucent 4645 Voice Messaging Services**
- Benefit from a contact center (**Alcatel-Lucent OmniTouch® Contact Center Standard Edition – OTCC SE**) that manages incoming voice interactions with advanced supervision and agent phone functions
- Enrich OTCC SE with omnichannel cloud services (email, chat, Facebook Messenger, Twitter, and phone call) to connect with your customers their preferred way with **ALE Connect***
- Eliminate costs associated with Fax machines, analogue lines, and consumables with the 100% Fax over IP (FoIP) software solution, **Alcatel-Lucent OpenTouch Fax Center**
- Monitor, record and evaluate all interactions between employees and customers, or patients with **Alcatel-Lucent OmniPCX® RECORD**, which allows you to record calls and screen captures and listen to conversations in real-time
- Enable your teams to define notification and alert strategies with the **Alcatel-Lucent Visual Notification Assistant** "no-code" interface: Notification by email, SMS, chat, using **Rainbow™ by Alcatel-Lucent Enterprise**, mass merging and audio diffusion on Alcatel-Lucent and third-party phones
- Equip your PC/MAC with all the functions of a desktop phone with the **IP Desktop SoftPhone** app
- Use desktop phones adapted to your needs from our large range of ergonomic phones with high-quality sound

* Selected countries (Western Europe)

Communications services for patients

Optimise the hospital welcome and offload the healthcare units

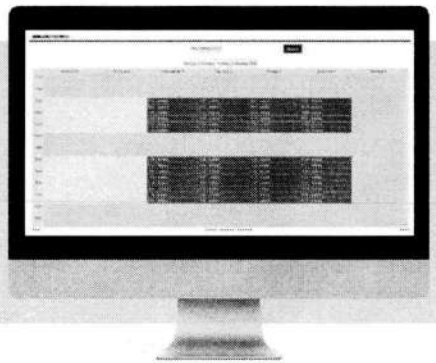
- Automate the most repetitive and resource-intensive tasks with an intuitive and economical interactive voice server, integrating voice synthesis and automatic speech recognition services

The ✪ of Visual Automated Attendant

- Easy creation and modification of routing scripts and voice guide by non-specialist users
- Welcome service professional image and response
- Standardised and differentiated welcome between healthcare units

Welcome 2.0 with "Click-to-Connect"

- No longer drop patients' calls: A simple web-based appointment solution provides automatic call back
- Optimise the facility's reception by offering intelligent routing to an agent, based on competence criteria (such as choice of pathology, or language) with multimedia management (chat/audio/video)
- Remove any doubt by activating video on the patient's smartphone without having to download an app



Make it easier for patients to communicate while they are hospitalised

- VIP patients and their relatives require high-end hotel style rooms and services, such as monitoring of their in-room comfort features (temperature, lights, ventilation and shutters) and access to hospital services (such as the hairdresser, or laundry). ALE provides the 8088 tactile handset running on Android, allowing partner apps to integrate their solutions into a high-end bedside handset.
- We also meet your specific needs such as provisioning of analogue or SIP handsets with antibacterial plastic adapted to the healthcare environment. Contact us for further details.

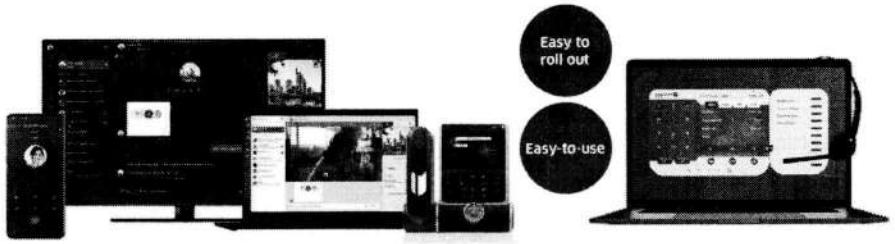
Maintain contact with patients at their homes

- Complete remote consultations, perioperative, or chronic illness monitoring with audio, video, or chat connectivity
- Optimise your resources by connecting the patient to a chatbot
- Monitor your patients' health conditions using IoT
- Connect your patients to an enriched virtual assistant with "Machine Learning" (chatbot/AI) enabling patient data analysis. With improved patient knowledge, the virtual agent can refine recommendations and, if necessary, make quick decisions such as triggering an alarm.

Alcatel·Lucent Enterprise

Make remote working easier for administrative staff

The global health crisis has highlighted the importance of innovative telecommunication strategies for remotely coordinating activities to ensure continuity of the healthcare facility, all while safeguarding individual's health data. Three solutions have proven to be effective and relevant:



Collaboration tool (Rainbow) | Remote ALE fixed phone | VoIP Softphone (IP Desktop Softphone)

IQ Messenger: A certified medical device alarm and notification solution

- Connect and monitor your clinical assets (such as patient monitor, or infusion pump) and smart objects. Reduce fatigue among healthcare staff due to the increase in the number of alarms
- Generate alarms from ALE DECT and VoWLAN handsets
- Send secure and reliable notifications on the DECT/VoWLAN handsets and smartphones (iOS/Android OS) from the SmartApp or Rainbow app

The ✪ of IQ Messenger

- Certified solution: ISO/IEC 27001, ISO 13485 and European MDR class IIb regulation on medical devices
- Extended clinical ecosystem: Integrated with more than 140 third-party provider systems
- Web and intuitive events flow manager

Cybersecurity

OmniPCX Enterprise

- Geographic hot redundancy
- Common Criteria EAL2 + renewal in process
- Built-in security with hardened operating system
- Security policy for voicemail users to avoid PBX fraud
- Confidentiality and integrity of voice media against wiretapping and IP Phone signatures, and media-gateways against denial-of-service attacks (IPSec)
- Mutual authentication against spoofing attacks
- Regular software update policy in order to benefit from the latest patches and upgrades

Rainbow

- Secure by design, reinforced by ALE conformity with the General Data Protection Regulation (GDPR), ISO 27001, and HDS, as well as audits by independent players (Nmap, Nessus Cloud, Qualys SSL Labs)
- Confidentiality and integrity of sensitive data with encrypted media flows in transport and in storage

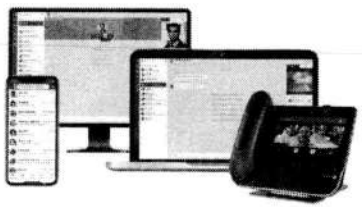
Innovation and integration

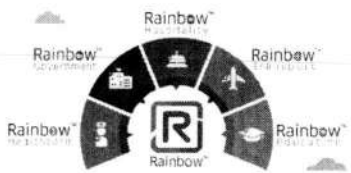
Integrate connectivity into business applications, clinical and operational procedures, and the ecosystem with the ALE OXE (O2G) and Rainbow API, as well as our technological components (such as IoT Hub, Rainbow Workflow):

- Provide communications from the Web portal: click-to-call, video, and presence
- Add audio, video, and chat, to business applications (PC/mobile), such as shared and computerised medical records
- Connect your application in a secure manner with a variety of IoTs, chatbots and Artificial Intelligence (AI) through Machine Learning (ML) technology
- Perform administrative operations: Synchronisation of an HR directory to create, modify, or delete the hospital's employee accounts

Value proposition for end-customers

- **Speed up your digital transformation** through truly mobile cloud-based communication, intuitive user collaboration, seamless deployment, and consistent design that boosts user-adoption
- **Leverage investments and connect your telephony system** with no rip-and-replace requirements. Rainbow offers a hybrid cloud that leverages your investments in PBX telephony systems by easily connecting them to the cloud and providing unified presence, desk phone click-to-call and softphone capabilities, and multimedia conferencing
- **Increase business process productivity** through the Rainbow Developer Hub. A Communications Platform-as-a-Service (CPaaS), the Hub provides integration capabilities into existing business applications, web sites, mobile apps, and workflows through various APIs and SDKs.
- **Flexible pricing models adapted to your needs** with usage or per-user subscription levels for audio conference. Pay-as you-grow with API consumption on the Developer Hub.





Rainbow service plans

Rainbow Essential: This free option is available to anyone who wants to try Rainbow for an unlimited period (no SLA). The Essential subscription can also be blended with any premium subscription, optimizing the cost of the solution for the whole organization.

Rainbow Business: The per-user subscription addresses individuals and teams who want to improve their daily communication, on- or off-site, on-the-move, or as a productive remote worker.

Rainbow Enterprise: The per-user subscription includes all services from Rainbow Business, but with the addition of collaborative multi-party services with video conferencing and extended file storage. Integration into existing office tools such as Microsoft 0365 and Google Suite also forms part of this service plan.

Rainbow Enterprise Conference: This per-user subscription packages the Rainbow Enterprise service plan with unlimited phone conferencing minutes. The Rainbow Enterprise Conference user subscription is pre-paid yearly in advance (twelve months).

Rainbow Conference: An optional service proposed as a "pay-as-you-go" model for phone (PSTN) conferencing with a price-per-minute/per-connection. The organizer of the meeting can be a Rainbow Essential (freemium) user, or premium user with Rainbow Business or Rainbow Enterprise subscriptions.

Rainbow Connect: The per-user subscription addresses users of any Customer Relationship Management (CRM) application. The integration of the Rainbow functionality is provided using a specific connector dedicated to the compatible CRM application.

Rainbow Room: An optional per-room subscription proposed for meeting rooms equipped with large screens for communication and interaction with people inside and outside of the company. Additional hardware is required to equip the meeting room and ALE has audio and video hardware kits readily available.

Rainbow by Alcatel-Lucent Enterprise

Instantly connect and collaborate with your business community

New technologies are revolutionizing the way that we communicate and interact. For businesses, the desire to remain competitive and attractive while continuing to deliver superior customer experiences necessitates that we have professional, reliable, and connected business phones in place.

Rainbow by Alcatel-Lucent Enterprise™ is the cloud-based collaboration service from Alcatel-Lucent Enterprise that empowers organizations and individuals to connect and collaborate efficiently with colleagues, business contacts, and customers.

Whether handling project details, answering customer questions, or providing quick resolutions, your team can do it all through Rainbow. With instant messaging, high definition audio or video conferences, and seamlessly created collaborative workspaces or groups, participants can securely share large files and host web conferences on the fly.

Rainbow by Alcatel-Lucent Enterprise is the cloud-based collaboration service from ALE

Available on desktop, web, smartphone, and tablet, Rainbow's key collaboration capabilities connect all your employees regardless of where they are situated, making it the perfect solution for effective remote working.

Extremely simple to deploy, Rainbow protects your existing investments and provides encrypted communications and data storage in data centers located in high privacy-conscious countries.

Rainbow also offers unlimited customization capabilities with numerous Application Programming Interfaces (APIs) and Software Developer Kits (SDKs) open to any developer. Rainbow cloud services can be integrated into a website (for example, a customer portal to reach sales or support teams) or integrated into any mobile application to provide augmented interactions with end-customers.

Solutions Sheet
Rainbow by Alcatel-Lucent Enterprise

Alcatel·Lucent
Enterprise

Optional add-on plans

Audio conference

Price per user, per month/year
- Up to 1,200 PSTN participants, multi-bridge audio, secure communications
- Call-me-back in 180 countries
- Local dial-in numbers across 50+ countries
- Web interface, Microsoft Outlook plug-in
- Chat, file sharing, screen or application sharing

CRM connect

Price per user, per month/year
- For SalesForce, Microsoft Dynamics and ServiceNow applications
- Phone control with single call management
- Contact/incident screen pop-up (auto search, contact search and display)

Room

Price per room, per month/year
- Audio/video conferencing system for middle and conference rooms, fully and supporting Zoho and Zendesk
- Dedicated Rainbow app for Android TV box
- HD video and audio streaming
- Centralized room management
- Audio/video kits for huddle and meeting rooms

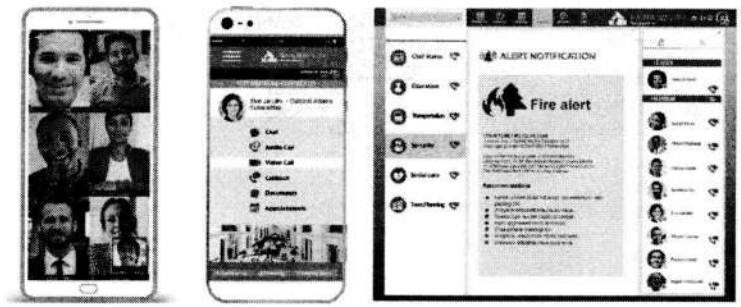
Increase business productivity

The Rainbow by Alcatel-Lucent Enterprise Developer Hub is an open CPaaS with a set of APIs and SDKs that allow any developer to integrate the powerful Rainbow collaboration tool into existing in-house applications, both web and smartphone based.

The Rainbow Hub makes digital transformation easy by providing extensive APIs, documentation, and support so that developers can build applications that connect people and transform the way they communicate and collaborate.

The service allows a developer to:

- Add real-time interaction and multimedia capabilities to any web or smartphone application
- Automate live interactions with AI-powered Bots and Chat Bots
- Integrate Rainbow with any customer's infrastructure or hardware (IoT)



The Rainbow Developer Hub offers more than 200 APIs, based on industry standards for chat, video, multimedia and provisioning services.

Find more information, check out our dedicated website for developers: http://hub.openrainbow.com

For more information about Rainbow Cloud Services, please visit our website: www.openrainbow.com

Alcatel·Lucent Enterprise

Service Plans

	Essential	Business	Enterprise	Enterprise Conference
Multi-platform client (Smartphone, Tablet, Web, PC, Mac)	●	●	●	●
Available in more than 75 countries and 20 languages	●	●	●	●
Collaboration				
Team collaboration (bubbles) with presence, chat, history search	● up to 20 participants	● up to 100 participants Multiple organizers	● up to 300 participants Multiple organizers	● up to 300 participants Multiple organizers
Company and public channels (broadcast news)	●	●	● Create and manage	● Create and manage
Persistent chat (peer-to-peer, group chat)	●	●	●	●
Presence information	●	●	●	●
Built-in voice and video communication, screen/app sharing	● peer-to-peer	● peer-to-peer	● 120 participants	● 100 audio participants
File sharing, storage	● 1GB of storage	● 1GB of storage	● 20 GB of storage	● 20 GB of storage
Call history		●	●	●
Recording (peer-to-peer)		●	●	●
Integration with office suites				
Click2Call connector for Google Chrome		●	●	●
Rainbow Telephony connector for Microsoft Teams		●	●	●
Calendar integration (Microsoft Office 365, Google Calendar)			●	●
Microsoft Outlook plug-in (includes contact search and web/audio conference scheduling)			●	●
Microsoft Office 365/Azure Active Directory (AD) contact search)			●	●
Connected PBX telephony				
Business phone control (with single call management)	●	●	●	●
Phone presence	●	●	●	●
Call logging	●	●	●	●
Any device (choose and control any phone)		●	●	●
VoIP calling (to PBX extensions, to public phone numbers)		●	●	●
Caller identification, user search		●	●	●
Second call management, 3-way call, call forwarding		●	●	●
Voicemail (visual interface, notifications, call)		●	●	●
Third-party PBX connectors (Avaya, Cisco, NEC, Mitel)		●	●	●
Security and compliance				
Region-based data residency	●	●	●	●
EU General Data Protection Regulation (GDPR)	●	●	●	●
Data encryption at rest and in transit (AES-256)	●	●	●	●
Single Sign-On (SSO)	●	●	● Administration	● Administration
Certified ISO/IEC 27001, 27017, 27018	●	●	●	●
ISO/IEC 20000-1 Information Technology Service Management	●	●	●	●
Certified Health Data Hosting (HDS) in France	●	●	●	●
Administration and Support				
Digital Help Center	●	●	●	●
Company administration and control	● 1 administrator	● Multiple administrator	● Multiple administrator	● Multiple administrator
Custom company logo, custom company banner	●	●	●	●
Analytics and reporting		●	●	●
Bulk user provisioning and deprovisioning		● CSV file	● CSV file, Azure AD	● 99% guaranteed uptime
Service Level Agreement (SLA) and Help desk (24/7 support with 20 mins first response time)		● 99% guaranteed uptime SLA	● 99% guaranteed uptime SLA	● 99% guaranteed uptime SLA

[redacted]

To the attention of Ms, Sir, [redacted],

Dear Madam, Ms, Sir,

Thank you for the time you have allowed us. Following your request, and after due study, we are pleased to submit you our best proposal regarding the project of an Alcatel-Lucent Enterprise communication solution in your company.

We trust that this approach will receive your fullest attention. Please do not hesitate to contact us for any further information.

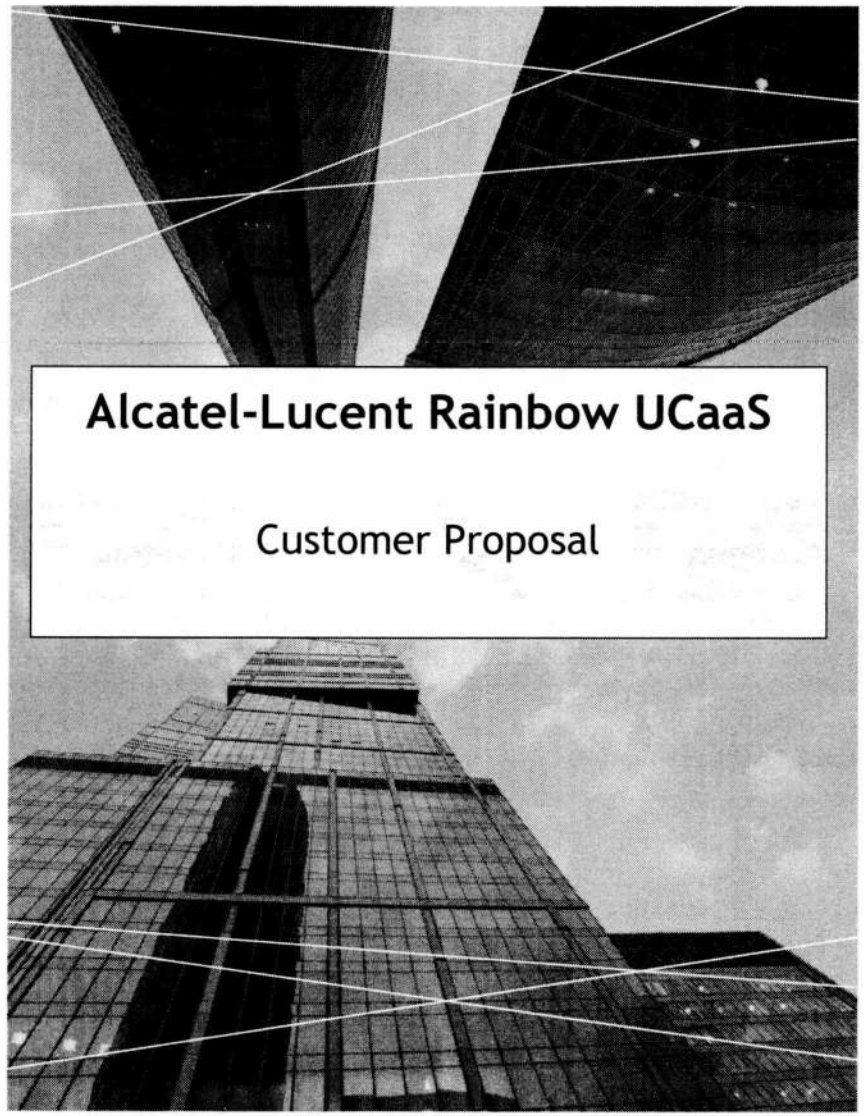
Thank you for your interest in our services, which we shall perform with the greatest care. We remain at your disposal to expand this budgetary quotation into a formal proposal including all your expectations.

Yours faithfully,

[redacted]

941

Alcatel·Lucent Enterprise



Alcatel-Lucent Rainbow UCaaS

Customer Proposal

Disclaimer: The information presented is subject to change without notice. ALE International assumes no responsibility for inaccuracies contained herein.

Table of Content

Alcatel·Lucent Enterprise

1
5
7

All Rights Reserved © ALE International 2020

1 Alcatel-Lucent Rainbow offer presentation

Alcatel-Lucent Rainbow™ is a **cloud-based**, **enterprise-grade**, Unified Communication as a Service (**UCaaS**) solution that connects people and systems.

Rainbow UCaaS services are available from any device: **desktop** (PC/MAC and Web), **smartphone** (iOS and Android), **tablet** (Android), **desk phone** (8088 Smart DeskPhone) and **meeting rooms** equipped with audio (speakerphone) and video (camera) devices.

With a **hybrid cloud** approach, Rainbow offers a global solution for business Collaboration and Communications with **connection to the customer on-premise PBX system.** Rainbow addresses the specific needs of our end-customers, from the small business requiring cost-effective mobility, to the multinational organizations that desires a single standard for unified communications across their complex IT, geography and along with the **integration in their business environment and applications (CRM).**

Rainbow can integrate with **ALE OXO Connect** and **OmniPCX Enterprise** products, but also with **3rd party IP PBXs** from different vendors (CISCO, AVAYA, NEC, MITEL).

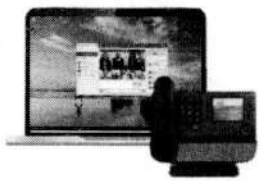
2 Value proposition of Rainbow UCaaS

The benefits of the **Alcatel-Lucent Rainbow** services are to:

- **Accompany your transformation to the cloud** - providing communication mobility, business community openness, click-to-deploy, ease of use and viral adoption
- **Secure your installed telephony system** - No rip & replace, hybrid cloud leveraging your investments in PBX telephony systems by connecting them easily to the cloud, and providing unified presence, click-to-call from desk phone, multimedia conference and more...
- **Integrate into your business environment** - Rainbow API Hub, a Communications Platform as-a Service (CPaaS), provides integration capabilities into the customer's business processes, web sites, mobiles apps and workflows through various sets of APIs and SDKs, including services from their own existing PBX infrastructure
- **Provide a subscription model for cost optimization & flexibility** - Price per user service, pay for what you use in conference

A true business app on your mobile:
Make the most from every call

Ultra-mobile business communications



Expert call management:
Serve customers faster and boost satisfaction

Engaging experiences with customers

Secure, connected platform:
100% on-premise, cloud, and hybrid options

A smooth transition to the cloud

3 Features overview

In this section you will find a high-level description of some of the main features provided to Rainbow users. The availability of the feature or service may depend on the user subscription (Service plan).

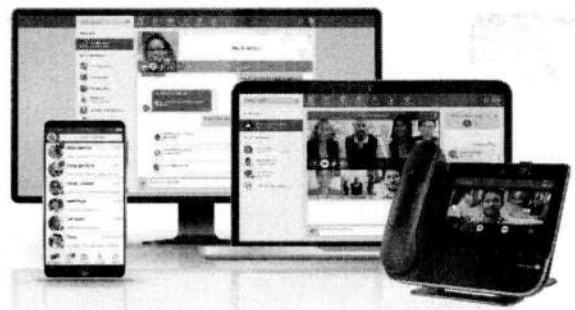
For a complete description of the solution and all functionalities available in the current release, please refer to the official Rainbow Feature List document.

You can refer to the description of the different user subscriptions in the section ***"Business model and Service plans"*** of this document.

3.1 Multi-platforms device software client

The Rainbow UCaaS cloud services are available whatever the device of choice of the customer:

- **Desktop:** PC Windows, MAC OSx, Web based client
- **Smartphone:** Android and iOS
- **Tablet:** Android
- **Desk phone:** 8088 Smart DeskPhone
- **Meeting room:** Dedicated Android app for compatible Android TV box



Whatever the device it offers a similar user experience for communications and collaboration purpose, in mobility, with the colleagues and beyond the corporate borders, with a rich integration into the legacy telephony system thanks to the connection to the corporate IP PBX.

There is no need for VPN connectivity between the device and the Rainbow cloud infrastructure, only an Internet connection is required.

There is no need for any adaptation at the level of the corporate LAN (e.g. firewall equipment) as the Rainbow client application uses standard communications protocol WebRTC. See the section ***"Pre-requisites and Compatibility"*** in this document for more information.

3.2 Collaboration services

3.2.1 Contacts

Once the Rainbow users have created an account and are connected to the client application on the device of their choice, they can instantly invite contacts to join their business community, start business chat or multi-party conversations.

3.2.1.1 Invitation

Invitation to contacts can be based on:

- Email (contact will receive an email inviting them to join Rainbow)
- Microsoft Outlook contacts
- Microsoft Office 365 contacts
- Google contacts
- Phone number (for mobile number only, contacts will receive a SMS inviting them to join Rainbow)

3.2.1.2 Search contact

It is possible to search a contact in:

- The user member list (personal network)
- The organization (including branches)
- Other companies (public members)

The user can search for business contacts (such as prospects, customers, suppliers) in the company's Rainbow Business Directory (managed by the administrator). It is also possible to search for a contact in the PBX phone book, Microsoft Azure Active Directory (if configured by the company) or in Microsoft Office 365 Global Address List (GAL).

For mobile users it is possible to search for local contacts stored in the mobile device.

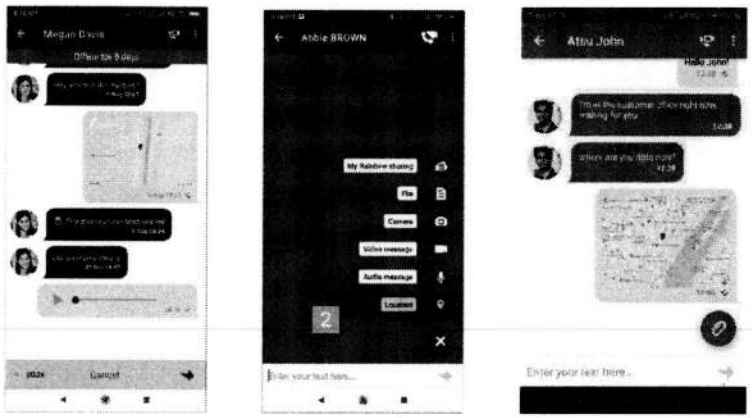
The administrator of the company can configure **'tags'** that are skills or properties (e.g. department, expertise, ID number, roles) assigned to the members of the company. Each user can have several tags assigned to the profile to facilitate people search.

3.2.2 Team collaboration

A Rainbow **bubble** is a workspace designed to meet the needs of real-time collaboration between Rainbow users (same company or several companies) or external guests. This group is created around a collective interest such as a project, a meeting, a presentation or a specific product. Like multi-user chats, bubbles open a special arena for real-time communication and collaboration.

The organizer of a Rainbow bubble can:

- Add/remove participants (same company or other companies)
- Invite an external guest (non-Rainbow user) based on an email address
- Share the URL link of the bubble to invite people (copy/paste in an email or calendar invitation), including external guests (no sign-in required), with privacy access mode

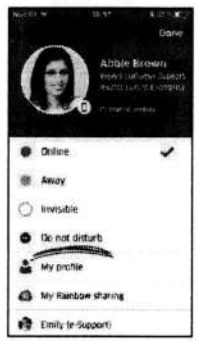


3.2.5 Presence

The Rainbow users can share their real-time availability information other Rainbow contacts and reduce the time spent blind-calling colleagues and coworkers. There are several predetermined presence options that can be selected manually, or that are updated automatically.

Presence states are as follows:

- Online: available to contact
- Mobile connected only: available to contact on mobile only
- Away: away for a period of time
- Busy: engaged in a call (audio or video) or sharing a content
- Do not disturb: don't want to be interrupted
- Invisible: want to be seen as offline
- Offline: not signed in



3.2.6 Calendar information

Calendar information is based on Microsoft Exchange Online with Office 365 or Google Calendar. The user needs first to authorize Rainbow to access your Office 365 or Google account (read access only).

- Promote/demote a participant to the organizer role to help managing or transferring the ownership of the collaboration space
- Transfer ownership of the bubble to another organizer of the bubble
- Initiate a meet-now multimedia call (audio, video and screen sharing). Note: this feature is available from the Rainbow Enterprise service plan

Depending on the level of subscription, a user can create a Rainbow bubble and invite up to 300 participants.

3.2.3 Conversations

A conversation between Rainbow users can be:

- a one-to-one conversation: Start peer to peer conversations with other Rainbow users
- a multi-party conversation: Use conversation rooms (bubbles) to share information with Rainbow and external guest users

The user can manage multiple conversations in a single view within the client application:

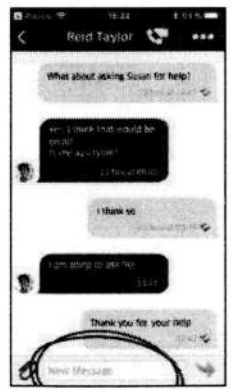
- Use audio, video, chat, screen/app sharing and file sharing in one-to-one conversations
- See calls made or received in one-to-one conversations
- Record one-to-one conversations
- See files you have shared in one-to-one or multi-party conversations
- Search for text in individual or multi-party (bubbles, meetings) conversations
- On the smartphone application: send messages when the mobile network connection is unavailable or intermittent

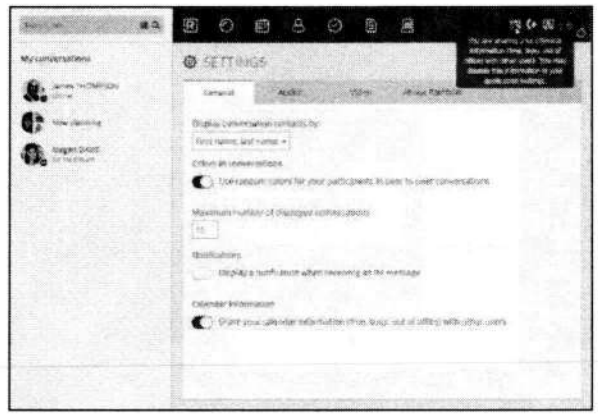
3.2.4 Instant messaging

Whether it's with one person or with a group, chat can help the user make decisions and take immediate action. And if the user happens to be idle, pop-ups will come to his device.

The Rainbow user can:

- Initiate a persistent chat with a Rainbow contact
- Send instant messaging within a Rainbow bubble for group chat
- Copy chat content
- Send all messages by email
- Remove all messages
- Use emoticons
- Use animated GIFs
- Use spell check
- Answer with chat to a voice or video call invitation
- Record and send vocal messages
- Share geo-localization (GPS) from mobile device





3.2.7 File sharing and storage

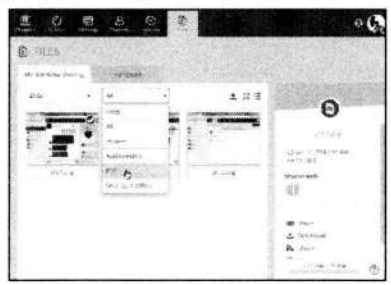
Rainbow users can save any file in their private Rainbow storage. Users can share pictures, documents or any other kind of file with people attending a conversation (one-to-one or multi-party).

With the Rainbow mobile application client, it is possible to share files (including audio and video files) from anywhere (with any contact or conversation, in your personal storage space) using the native iOS share extension or native Android share extension.

A user can send multiple files at once from the desktop client:

- From the computer or personal Rainbow storage space into conversations
- From the computer to the personal Rainbow storage space

A user can get a quick access to files received and sent. Sender of the files is identified and who can see the files that have been sent. Files are sorted by date, by name or by size. The user can manage the personal storage space and suppress one, several or all files at a time.



3.2.8 Screen and application sharing

Rainbow users can share their screen by starting a conversation with one or several people (within a Rainbow bubble). Participants will see the sharing from the device of their choice (desktop, Web, smartphone), in normal or full screen mode.

Rainbow users can also share a specific application from their desktop, to avoid other people to see anything else from the computer.

3.2.9 Channels

Any Rainbow user can benefit from the Channel feature to broadcast information to a group of persons within or outside of the company. For example, a business owner, or secretary or marketing person can invite people to dedicated channels, such as HR, company news, etc.

It's a great way to promote internal news, links, documents or videos.

Zero coding skills are required to publish a post. The posts are sent to all, mobile workers, telecommuters, office workers. When they sign-in to Rainbow, the channel tab is the first information they see!

The Rainbow Channel feature can be used to replace an aging intranet website that's too complex to update and rarely viewed by the employees of the company.

There are 2 kinds of channel:

1) **Company** means you can share information with people of your company only
2) **Public** means you can share information with people outside of your company. It is restricted by an administrator right (all people of a company will not be able to share information off the company)

3.2.11 Call recording

Rainbow users can record the audio and either the video or content sharing (screen/app) of individual web calls, e.g. to recall exact content and wording, improve customer service and satisfaction, avoid disputes or misunderstandings.

The records (MP4 files) are saved either in the personal Rainbow storage space or on the computer.

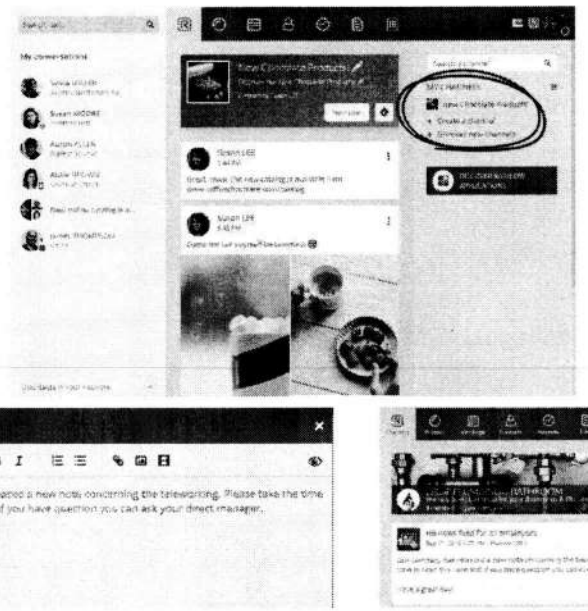
Note: when a recording is started, recorded user receives a beep and a visual indicator is displayed. User can stop the recording anytime (by ending the conversation) when being recorded without its consent.

3.3 Business telephony services

3.3.1 Leverage the investment in existing telephony system

Rainbow connects natively with the recent ALE OmniPCX Enterprise, OXO Connect/Evolution systems of the customer installed on-premises. The phone system just requires an Internet connectivity to the Rainbow cloud services. This network connectivity is encrypted and secured.

In a large company, with multiple subsidiaries and remote sites, Rainbow can federate the different phone systems to provide unified communications to all employees with a unique client application and user experience. Rainbow makes it easy for all the company workers to see the on-the-phone status of colleagues, perform a directory search and escalate their phone calls to video or screen sharing with internal or external people.



3.2.10 Call history

Call history shows information about the audio conversations (latest 75 items are displayed). Conversations are listed chronologically from the most recent call to the oldest one. Calls are grouped by contact.

Rainbow users can manage their call history:

- Show the recent calls
- Delete a history record / all records
- Show conversation details
- Check sent and received files
- Sort the call history
- Filter the call history
- Missed calls indicator

3.3.4 Ubiquity for all made easy with Rainbow

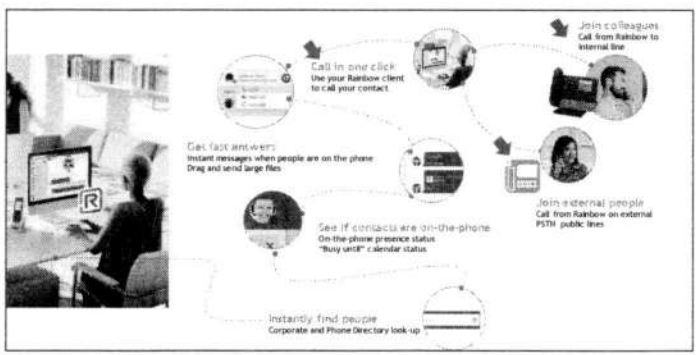
The Rainbow user also benefits from a nomadic mode to control any other phone, whether fixed or mobile, in addition to the business phone. This is very useful for mobile, on- or off-site employees as well as home workers using their personal home phone for audio calls.

Rainbow for mobility: fix/mobile convergence and teleworkers

3.3.5 Softphone for all made easy with Rainbow

Rainbow offers a unified multi-device experience between the desk phone and the mobile phone, and a pure softphone experience with VoIP for the end-user.

Thanks to the additional software component Rainbow WebRTC Gateway, that connects to the on-premise ALE Communications Server (OmniPCX Enterprise or OXO Connect/Evolution), making calls available from any device has never been so easy. The Rainbow WebRTC Gateway brings voice media between the Rainbow client on desktop (or mobile) and the corporate Communications Server, including business phones (IP, digital, analog, DECT) and PSTN accesses.



Business calls with the device of your choice

3.3.2 Desktop phone companion

When the corporate telephone system is connected to Rainbow - the perfect companion for the business desk phone - it results in a great user experience.

The user can:

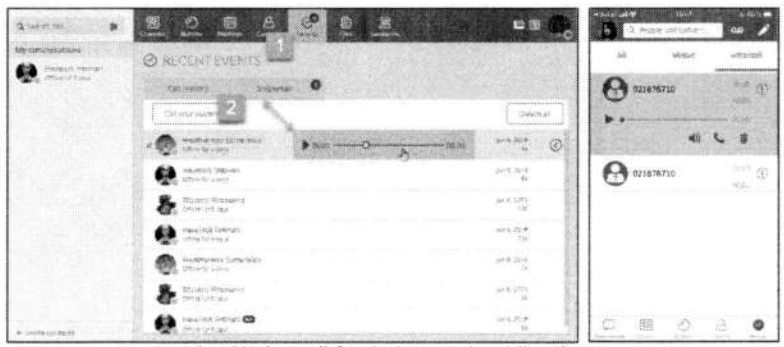
- access to the corporate address book
- see the on-the-phone presence status of contacts
- launch click-to-call to contacts
- see the call log for passed and missed calls
- manage call routing (deskphone, mobile, tablet, computer VoIP)
- manage voicemail

3.3.3 Voicemail system integration

For companies connecting their existing Alcatel-Lucent Enterprise OmniPCX Enterprise or OXO Connect/Evolution Communications Server to Rainbow, it provides the possibility for the user to access and manage voicemail messages directly from the Rainbow client interface.

The user receives notifications in case of new messages and can be connected to the voicemail system with the Telephony User Interface (TUI). This also allows the user defining or changing, for example, greetings and personal options.

For company with OXO Connect/Evolution Communications Server, it is possible to activate the visual voicemail feature for users with the desktop or mobile client. The visual voicemail in the Rainbow client allows to display and manage the voice messages: select, play, delete. Voice messages are also archived in the Rainbow personal storage space, so the user can download, transfer or delete them.



Visual Voicemail for desktop and mobile clients

3.4 Phone Conferencing service

Rainbow offers a phone conferencing service for up to 100 participants available from any phone over PSTN all over the world (check the country list availability).

Each user has a personal conference bridge and can also easily schedule a meeting including the phone conference details via the Microsoft Outlook Calendar add-in. All guest participants benefit from collaboration features such as instant messages, file sharing, screen sharing.

This service can be used anytime, anywhere, and on any device (internal or external line, landline or mobile), enabling both employees and external contacts to join a phone meeting. Rainbow users can set up a meeting quickly using this phone conferencing service, eliminating the need for IT resource support.

In the table below, you can see a highlight of the main characteristics of the Rainbow Conference option:

Phone Conferencing service	
User interface in the Rainbow client	
Maximum number of participants	100
Mode of communication	Local numbers in 60+ countries
Call Detail Record (CDR)	YES
Media	Audio (phone over PSTN), Instant Messages, Screen Sharing
Instant/Scheduled meetings	Personal conference bridge
Add guests (non-Rainbow users)	YES
Integration in office suites (MS Outlook, GSuite) **Add URL of the conference bridge into the invitation**	YES

You can refer to the description of the different user subscriptions in the section **"Business model and Service plans"** of this document.

With Rainbow a user can easily collaborate with colleagues or external people:

- First instantly find people
- then see if the contact is busy or available
- get fast answer with instant messages
- call in one-click a contact from the Rainbow client
- join an external person via PSTN from the Rainbow client application using VoIP and establish easily a multiparty conference

3.3.6 Rainbow connector to third-party PBX

Companies with a heterogenous network and telephony systems from different vendors (other than Alcatel-Lucent OmniPCX® Enterprise or Alcatel-Lucent OXO Connect/Evolution) usually struggle to provide a unique and federated UC (Unified Communications) solution for all employees. Thanks to the Alcatel-Lucent Rainbow® connector for third-party PBX, they can now federate all users and provide a homogeneous level of service with instant messaging, file storage and sharing, audio and video conferencing, team collaboration, and integration with the existing telephony system via CTI (Computer Telephony Interface).

Connecting a third-party PBX to Rainbow cloud services allows users to benefit from the Rainbow client application (on PC Windows/macOS/Web) to control business phone calls from/to phone sets connected to the third-party telephony system.

3.3.6.1 PBX models supported by the Rainbow connector

The Rainbow connector for third-party PBX is available for:

- Avaya IP Office 500 V2
- Cisco Unified Communications Manager versions 9.x, 10.x, 11.x and 12.x.
- NEC UNIVERGE 3C
- Mitel MiVoice 5550/5540, MiVoice Business Virtual, MiVoice Office

3.3.6.2 Level of business telephony services

Main features provided by the Rainbow connector for third-party PBX:

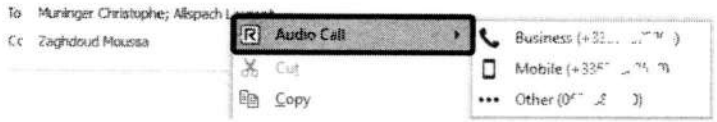
- Caller identity
- Telephony presence status (online, busy)
- Business telephony services: Simple call, second call, three-party conference
- Search contact from PBX phonebook
- Missed call notification, call log

3.3.6.3 Associated user subscription

Rainbow users with a phone set connected on the third-party PBX need a Rainbow Business, Enterprise or Enterprise Conference subscription.

TAPI and other PBX specific licenses may be needed for CTI monitoring and telephony events.

TSP software is required for AVAYA IP Office and CISCO Unified Communication Manager.



3.5.2 Microsoft Teams integration

Rainbow complements (via an additional PowerApp and light desktop app) Microsoft Teams collaborative workplace with enterprise telephony system integration and phone presence information. Thanks to this desktop-based integration, organizations that have deployed Microsoft Teams for instant messages and presence will benefit from Alcatel-Lucent Enterprise business telephony extensive features set and reliability, as well as comfortable audio on desk phones and wireless phones (VoWLAN or DECT).

Two applications as add-in are required:

- A PowerApp within Teams
- A light desktop app for managing events and calls

The main features provided are:

- **Via the PowerApp**
  - Rainbow authentication
  - Selection of the current phone
  - Call forwarding
  - Call history
  - Voicemail (call, notifications)
- **Via the smart desktop app (Rainbow icon in Windows notification area)**
  - Management of single calls (answer call, end call, clear call)
  - Notification of new events (missed calls, voice messages)
  - Hotkey dialing anywhere on your desktop

3.5 Microsoft Office Suite integration

3.5.1 Microsoft Outlook integration

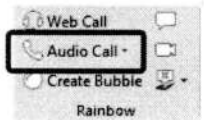
The Rainbow add-in for Microsoft Outlook can be installed to complement Rainbow client application on the desktop with audio (web calls and phone calls), video, chat, screen share and meeting scheduling including phone conference.

The Rainbow add-in for Microsoft Outlook can be connected to an on-premise Microsoft Exchange Server or to the hosted service from Microsoft (Exchange Online standalone service or as a part of Microsoft Office 365 offer).

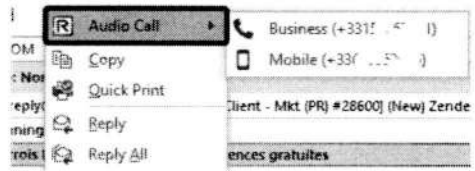
Below is a non-exhaustive list of services provided when the Rainbow add-in for MS Outlook is configured:

- Communicate with the sender/recipients of an email: start a conversation (audio, video, phone, chat, screen share etc.)
- Start an audio call: using the computer or the business phone
- Start a video call
- Start a chat
- Communicate with a Microsoft Outlook contact
- Create a Rainbow bubble from an email to invite all recipients as members
- Schedule a meeting and add URL of a Rainbow bubble for instant video conference (based on WebRTC)
- Schedule a meeting and add URL of the phone conference (requires that the phone conferencing service is granted to the Rainbow user)

Select an email or a contact and click the Audio Call button in Home tab ribbon:



Or right-click an email or a contact and use the Rainbow Audio Call action:



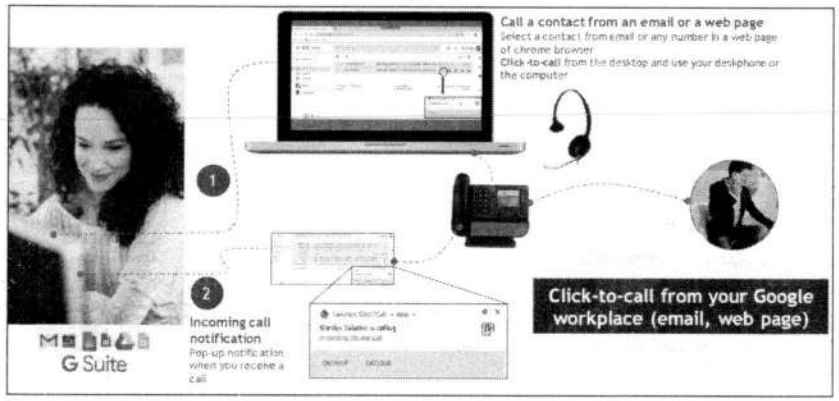
Or start a phone conversation with any recipient of an email. Right-click the recipient and use the Rainbow Audio Call action:

Chrome and right-click to place a phone call

- Call forwarding: forward all calls to the user voicemail or to a phone number

A user can add the Rainbow Click2Call extension to the Chrome browser by downloading the extension from the Chrome Web Store.

Administrators can automatically install (force-install) the Chrome extension for users in your organization (users then see the extension when using Chrome on managed devices or accounts) by managing Chrome policies from the Google Admin console.



Rainbow integration within Google Suite

3.7 CRM applications integration

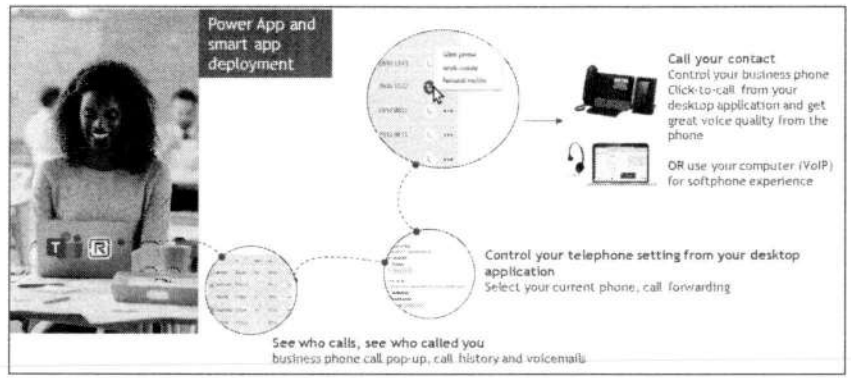
The Alcatel-Lucent Rainbow™ CTI connector for CRM applications provides an easy to use business phone (or softphone) from the desktop, and smooth integration with the Alcatel-Lucent OmniPCX® telephony platforms.

The Rainbow CTI connector is a complete solution that allows the CRM desktop user interface to receive information about the caller when the business phone rings, and it offers a click-to-call function from the CRM contact card.

CRM applications users need a quick and efficient way to reach prospects by phone. A Computer Telephony Integration (CTI) solution removes the need to manually dial the business phone, which can be slow and cumbersome. Telephone numbers associated with any CRM object such as, leads, contacts, and cases turn into clickable links, which the user can leverage to place outbound calls using the ALE business phone, or softphone.

With the Rainbow CTI connector, the CRM use benefits from:

- Click-to-call a CRM contact through the existing telephony system for public number
- CRM contact card pop-up on incoming call
- Rich presence of other CRM agents with telephony integration
- Agents contacts list based on Rainbow Directory



Rainbow integration within Microsoft Teams

3.6 Google Suite integration

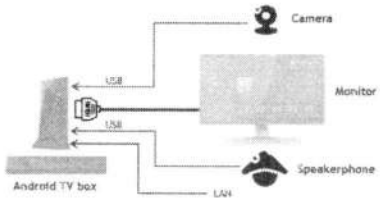
Rainbow complements the Google Suite collaborative workspace with business telephony services thanks to a Chrome extension:

- Select the device you want to use for managing phone calls
- Initiate calls from Google Gmail or from any Chrome web page
- Manage your call routing

The main features provided are:

- Desk phone control: the user can control and monitor the desk phone from the desktop
- Control any phone: the user can manage phone calls from this phone, while keeping a unique identity. The function is available for users having a desk phone as main business line with a tandem/multi device configuration, or users without a desk phone
- VoIP calling: the user can make (or receive) phone calls to (or from) PBX extensions and public phone numbers from anywhere by using the computer for VoIP. The function requires the Rainbow WebRTC Gateway installed on the customer telephony system (om-premises or hosted)
- Incoming call "twinning" (simultaneous ringing): ring simultaneously the computer or any other device (e.g. personal mobile, home phone) and the user's business communication devices (e.g. desk phone, DECT handset) to ensure never miss an important call. Calls can be answered by either device
- Caller identification: identification of a calling party (with UTF-8 support) is based on the Rainbow directory (phone numbers in E.164 format) or the PBX phone book
- Call the sender of an email from Google Gmail app: from Google Gmail application, quickly call the sender of an email if sender is a Rainbow user. Select the number to dial if the sender owns several phone numbers
- Call a phone number from any Chrome web page: Select any phone number from Google

- A **Rainbow Room subscription** (monthly or annual)
- A compatible **Android TV box** connected to the meeting room **monitor** via HDMI
- An **Internet connection** for the Android TV box
- The **software application Rainbow Room** installed on the Android TV box
- A **camera** connected to the Android TV box via USB
- A **speakerphone** connected to the Android TV box via USB



Key features	Customer benefits
Online video conferencing	Simplify meetings with guests and have external people joining in one-click from any compatible web browser.
Visual collaboration	Make distant meeting natural with video, file and screen sharing: invite up to 50 participants per conference and enjoy quality time with them wherever they are.
Global presence	Alcatel-Lucent Rainbow global presence offers excellent meeting quality whatever the distance, even if you have suppliers or customers overseas.
Secured communications	Alcatel-Lucent Rainbow uses state-the-art WebRTC audio and video for secure communications leveraging your Internet access.

Rainbow Room for equipped meeting rooms

- Conversation with other connected agents: instant messages, file sharing
- Audio and video* call with connected agents

(*) features capabilities may depend on the CRM application

Rainbow integration within CRM applications

The Rainbow CTI connector is available for below configurations:

- **CRM applications:**
  - Salesforce Sales Cloud and Service Cloud
  - Microsoft Dynamics CRM
  - ServiceNow ITSM
- **Telephony systems:**
  - OmniPCX Enterprise R12.2 or higher
  - OXO Connect R3.x or higher

3.8 Rainbow Room

Rainbow Room is a subscription that empowers individuals and teams to connect and collaborate efficiently with colleagues, business contacts and customers. It is dedicated to meeting rooms equipped with a large screen for communication and interaction with distant people.

To benefit from the Rainbow Room features, the elements listed below must be provided for one meeting room:

4 Security, Data privacy and Compliance

Alcatel-Lucent Rainbow is an enterprise-grade cloud service operated by ALE, a recognized enterprise expert.

Security in the cloud is sometimes identified as a barrier to adoption. Privacy and the reliability of Cloud services are also questioned, so customers need reassurance! Rainbow offers a strict data privacy policy with Data Centres in different locations for a worldwide coverage of the service. Rainbow has Points of Presence in privacy conscious countries such as France, Germany, USA, Canada, Singapore and Australia. Under the terms of the contract, personal user data is not used for commercial or marketing purposes, and ALE ensures a compliancy with local data privacy regulations such as GDPR in European countries.

Alcatel-Lucent Rainbow cloud services is certified ISO 27001. It means that ALE cloud teams are properly managing information risks to protect the security of our customers data. Customers can feel confident about the security of their data when doing business with ALE.

The Alcatel-Lucent Rainbow cloud services offer multiple security-oriented features for the benefit of customers:

- Use of TLS 1.2, Secure HTTP (HTTPS), Secure RTP (SRTP), DTLS and XMPP over WSS (WebSockets over TLS)
- Firewall traversal and compliance with the latest standards (ICE, STUN and TURN)
- User password policy
- Secure self-registration for user account creation and secure password reset
- Single Sign-On (SSO) with SAML 2.0 and OpenID Connect. Rainbow also supports SSO with on-premises Microsoft Active Directory thanks to the Active Directory Federation Services (ADFS) role, using either SAML 2.0 or OpenID Connect.

For more information refer to our official documentation **ALE Rainbow Solution Brief** regarding security:

https://support.openrainbow.com/hc/en-us/articles/115001019330-Solution-Brief-Security

5 Pre-requisites and Compatibility

Device compatibility

Rainbow is available for desktops (web browsers and PC Windows/MacOS apps), smartphones and tablet.

Please check the Feature List/White List information available in our Rainbow Support website:
https://support.openrainbow.com/hc/en-us/articles/115001057424-Feature-List-White-List

Network requirements

Rainbow is based on Internet services. You must have an active connection to Rainbow web servers.

Please check the Network Requirement Guide available in our Rainbow Support website:
https://support.openrainbow.com/hc/en-us/articles/115000301750-What-Are-Rainbow-Network-Requirements-

RAINBOW SERVICE PLANS	ESSENTIAL	BUSINESS	ENTERPRISE	ENTERPRISE CONFERENCE PACK
Mobility and Collaboration				
Multi-platform client (smartphone, tablet, Web, PC, MAC)	•	•	•	•
Contacts (individuals, groups, guests)	•	•	•	•
Voice and video calling/conference, with screen sharing	• 1-on-1	• 1-on-1	• Up to 50 participants	• Up to 50 participants
Call recording (1-on-1)		•	•	•
Team collaboration (bubbles) with presence information, chat history and search	• Up to 25 participants	• Up to 100 participants Manage multiple organizations	• Up to 250 participants Manage multiple organizations	• Up to 500 participants Manage multiple organizations
File sharing, storage	• 1 GB of storage	• 1 GB of storage	• 20 GB of storage	• 20 GB of storage
Channels (broadcast news)	•	•	• create and manage	• create and manage
Integration with Office Suites				
Click-to-call extension (Microsoft Teams, Google Suite)		•	•	•
Microsoft Outlook plug-in, incl. click-to-call, contact, add URL to conference in appointment			•	•
Calendar information (Microsoft O365, Google Calendar)			•	•
Microsoft Azure Active Directory (AD) contact search			•	•
Hybrid Cloud Telephony				
Business phone control (with single call management)	•	•	•	•
Phone presence	•	•	•	•
Call logging	•	•	•	•
Any device (choose and control any phone)		•	•	•
VoIP calling (to PBX extensions, to public phone numbers)		•	•	•
Second call management, 3-way conf, call forwarding		•	•	•
Voicemail (visual interface, notifications, cast)		•	•	•
Third-party PBX connectors (Avaya, Cisco, Mitel, NEC)		•	•	•
Management and Support				
Company administration and control	• Last Administrator	• Multiple administrators	• Multiple administrators	• Multiple administrators
Analytics		•	•	•
User provisioning and deprovisioning		• CSV file	• CSV file, Microsoft Azure AD	• CSV file, Microsoft Azure AD
Digital Help Center	•	•	•	•
Service Level Agreement (SLA) and support/help desk		• 99.5% guaranteed uptime SLA	• 99.5% guaranteed uptime SLA	• 99.5% guaranteed uptime SLA
RAINBOW CONFERENCE	Optional CONFERENCE (Pay as You Go)			Included
Audio Conference bridge access up to 100 PSTN participants with web interface for instant messages, file and screen sharing	priced / minute per connection type per participant			no additional cost
RAINBOW CONNECT	CONNECT			
Optional CRM connector service plan	priced /user /month, available also in yearly plans			
Supported CRM: Salesforce, MS Dynamics, Service Now	•	•	•	•
ALE phone control from CRM (with single call management)	•	•	•	•
VoIP calling to PBX extensions, to public phone numbers		•	•	•
RAINBOW ROOM	ROOM			
Rainbow service plan for small and large meeting rooms	priced /room /month, available also in yearly plans			

For a complete list of the services available with each service plan, please refer to the official Rainbow Feature List document available on ALE public website:

https://support.openrainbow.com/hc/en-us/articles/115001057424-Rainbow-Feature-List-and-Applications

6 Business Model and Service Plans

The level of service that is provided to a user depends on the subscription that applies to this user. Within the Rainbow UCaaS offer there is a freemium subscription, premium subscriptions and optional services.

Below is the detail of the Rainbow UCaaS offer:

Rainbow Essential: Free-of-charge, Rainbow Essential is available to anyone who wants to try Rainbow for an unlimited period (no SLA). The Essential subscription can also be blended with any premium subscription, optimizing the cost of the solution for the whole organization.

Rainbow Business: The per-user subscription addresses individuals and teams who want to improve their daily communication, on-site or off-site, on-the-move or as a remote worker. It is a monthly or multi-year (pre-paid for a period of one year, three years or five years) subscription.

Rainbow Enterprise: The per-user subscription includes all services from Rainbow Business, in addition to collaborative multi-party services with video conferencing and extended file storage, as well as office tool integration including: Microsoft 0365, Google Suite. It is a monthly or multi-year (pre-paid for a period of one year, three years or five years) subscription.

Rainbow Enterprise Conference: The per-user subscription packages the **Rainbow Enterprise** service plan with unlimited phone conferencing minutes. It is a pre-paid subscription for a period of one year (twelve months).

Rainbow Conference: An optional service proposed as a "pay-as-you-go" model for phone conferencing with a price-per-minute/per-connection. The organizer of the meeting can be a Rainbow Essential freemium user, or premium user with Rainbow Business, or Rainbow Enterprise subscriptions.

Rainbow Connect: The per-user subscription addresses users of any Customer Relationship Management (CRM) application. The integration of the Rainbow functionality is provided thanks to a specific connector dedicated to the compatible CRM application.

Rainbow Room: An optional per-room subscription proposed for meeting rooms equipped with large screens for communication and interaction with people inside and outside of the company. Additional hardware is required to equip the meeting room and ALE has audio and video hardware kits readily available.

The table below is a high level view of the main features provided to the user depending on the user subscription:

7 Pricing proposal

Rainbow Essential	free
Rainbow Business	X € / user / month or multi-year (1, 3 or 5 years)
Rainbow Enterprise	X € / user / month or multi-year (1, 3 or 5 years)
Rainbow Enterprise Conference	X € / user / year
Rainbow Connect	X € / user / month or multi-year (1, 3 or 5 years)
Rainbow Room	X € / room / month or multi-year (1, 3 or 5 years)
Rainbow Conference	: consumption-based model - refer to the price list per country

ANY QUESTION?

Please contact your reseller:

RESELLER NAME:

...

CONTACT:

...

End of the document

160

ALCATEL-LUCENT RAINBOW™

Network Requirements

GETTING STARTED GUIDE Ed 23

APRIL 2022

Author: Operations - Cloud Services

Alcatel·Lucent Enterprise

Contents

1 Introduction

Rainbow by Alcatel-Lucent Enterprise (ALE) is an overlay cloud service operated by ALE. Rainbow offers contact management, presence, persistent messaging, audio/video for peer-to-peer and multiparty real-time collaboration, screen and file sharing, telephony services on existing customers PBX or based on native cloud telephony capabilities, and API openness to integrate with customers processes, applications and machines.

Rainbow's clients and agents connect to Rainbow cloud services using Web protocols.

This document describes the high level principles of network flows implemented by the solution, provides detailed information on Rainbow network connectivity requirements, allowing network and security administrators to identify needed firewall rules, verify bandwidth availability, and tune intermediate security elements such as proxies when applicable.

Section 3.2 gives a short summary of requirements for readers who do not have advanced security infrastructure or rules in place, and don't need to dive into the details

2 Document History

Modifications (see last edition's changes in green)	Date	Edition
Addition of a summary paragraph for required flows for collaboration, Hybrid and Hub (section 3.2) Updated on WebRTC Gateway (section 4.6): • more relevant repartition of flows towards Rainbow Cloud and towards LAN side components • update on DMZ topology with dual interface capability Add note on TTL for NAT mappings for Android app connection to Google FCM service (section 4.2) Add new conference server IP in China	Xx/04/2022	Ed 23
Updated section 5 with FQDN and IP addresses changes related to: • add Webrtc and Turn located in Middle East/Bahrain • New external load balancers IP for Singapore WebRTC gateway: Add details on NAT configuration for UDP, deployment in the DMZ specificities and configuration of a DNS server is mandatory	04/02/2022	Ed22
Add new media relay servers IPs and names to whitelist Add new file sharing DNS entries Add webinar DNS entry Add connectors (teams...) IPs Precision of HTTP version supported by WRG (HTTP 1.1)	03/11/2021	Ed 21
Updated to notify removal of conference server number 4 in Brazil, turn server in Washington DC and Load Balancer in Washington DC	28/09/2021	Ed 20

Glossary

ALE:	Alcatel-Lucent Enterprise
PBX:	Private Branch Exchange
HTTP:	Hyper Text Transfer Protocol
HTTPS:	Hyper Text Transfer Protocol Secured
ICE:	Interactive Connectivity Establishment - RFC 5245
STUN:	Simple Traversal of UDP through NAT - RFC 5389
TURN:	Traversal Using Relays around NAT - RFC 5766
DTLS-SRTP:	Datagram Transport Layer Security - Secured Real Time Protocol

163

SDK specificities		
TURN endpoints update, bandwidth requirements update	04/07/2017	Ed 08
HTTP vs. HTTPS cleanup	04/04/2017	Ed 05
Minor change (legacy PBX Agent removed)	31/03/2017	Ed 04
Information on bandwidth added (chapter 6)	08/03/2017	Ed 03
Chapter **Erreur ! Source du renvoi introuvable.** modified	05/01/2017	Ed 02
Creation of document	27/10/2016	Ed 01

Addition of information for Teams and Google connectors Some fixes in WebRTC Gateway port ranges Some precisions on proxy dimensioning aspects Streamline document paragraph numbering		
Updated section 5.4 with FQDN and IP addresses changes related to: • Removal of now deprecated TURN SBG1 configuration • Updated DNS/IP information on mail servers.	04/03/2021	Ed 19
Updated section 5.4 with PBX Agent bandwidth	19/11/2020	Ed 18
Updates to cover Rainbow Room, Rainbow Hub, and refined information on video bandwidth after introduction of simulcast video	27/09/2020	Ed 17
Updated section 5.4 with FQDN and IP addresses changes related to: • turn.sbg1.openrainbow.com removal	28/07/2020	Ed 16
Updated section 5.4 with FQDN and IP addresses changes related to: • New ANZ region and associated servers • New EMEA load balancers servers	30/06/2020	Ed 15
Updated section 5.Edition4 with FQDN and IP addresses changes related to: • New EMEA TURN and Media Conferencing servers • EMEA TURN and Media Conferencing servers removal • New South America Media Conferencing servers • New DE Media Conferencing servers • DE Media Conferencing servers removal	21/04/2020	Ed 14
Updated section 5.4 with FQDN and IP addresses changes related to: • South America Load Balancer, TURN and Media Conferencing servers • Germany Load Balancer servers • Europe and North America mail servers • UK TURN and Media Conferencing servers (removal)	11/07/2019	Ed 13
Updated section 5.4 with complete list of public IP addresses Section 5.3.4: WebRTC Gw now supports crossing web proxy for media flows.	15/03/2019	Ed 12
Improve and complete IP flows information presentation; some doc reorg; precisions on bandwidth for mobile devices; new TURN server	10/01/2019	Ed 11
Extended WebRTC TURN endpoints configuration	11/14/2018	Ed 10
Video Bandwidth requirements update, WebRTC GW requirements and	05/17/2018	Ed 09

3.2 Summary of ports/protocols requirements

This section provides the basic information on outgoing flows to enable for Rainbow to properly connect to Rainbow infrastructure. Details on the rationale and on the way the solution works are provided in further sections of the document.

3.2.1 Rainbow Collaboration

The table below gives minimum requirements for deployment of Rainbow as a collaboration solution, without telephony services.

Protocol	Port	Main use	Source	Destination [a]
TCP	443	Signaling, APIs Messaging, filesharing	All Rainbow clients and applications	*.openrainbow.com openrainbow.com openrainbow.io
UDP [b]	3478	Audio/video/desktop sharing media	All Rainbow clients	*.openrainbow.com
TCP [c]	5228-5229-5230	Android push notif	Pure wifi Android devices	Google FCM servers
TCP	443	Apple push not	Pure wifi iOS devices	Apple APNS servers

(a) details on FQDN and IP addresses of Rainbow servers are provided in section 5

(b) the solution can fall back on TCP/443 if the infrastructure does not allow UDP (UDP remains highly recommended for best quality of service for multi-media flows)

(c) Google requires that if the network implements Network Address Translation (NAT) or Stateful Packet Inspection (SPI), a 30 minute or larger timeout is maintained for FCM connections over ports 5228-5230

3.2.2 Rainbow Hybrid Telephony

The table below gives minimum requirements for deployment of Rainbow on top of an existing customer PBX, providing telephony services and optionally advanced collaboration services.

Protocol	Port	Main use	Source	Destination [a]
TCP	443	Signaling, APIs Messaging, filesharing	All Rainbow clients and applications WebRTC Gateway PBX	*.openrainbow.com openrainbow.com openrainbow.io
UDP [b][c]	3478	Softphony with remote users	All Rainbow clients WebRTC Gateway	*.openrainbow.com

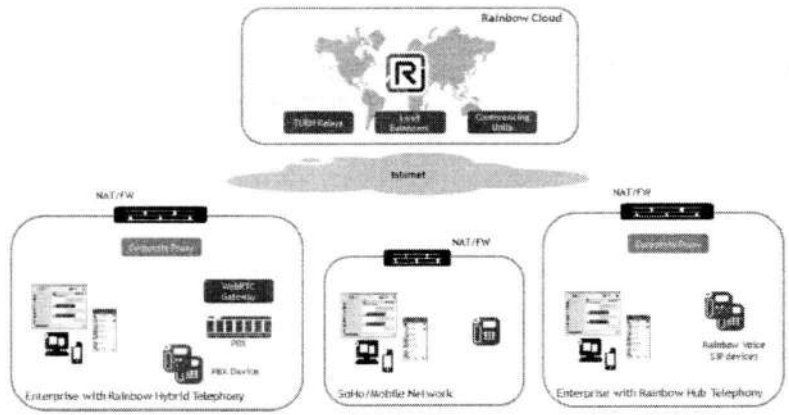
3 Solution Overview

3.1 Global Overview

The Rainbow solution provides multiple client-side applications to connect to the service:

- A Desktop application for Windows and OSX (Web-based, Electron-contained)
- A Web application for WebRTC compatible browsers
- An iOS native application
- An Android native application
- An Agent to connect customers' PBX for hybrid telephony (can be integrated with the PBX)
- A WebRTC Gateway to establish multimedia calls between customers' PBX and Rainbow
- Various SDKs allowing developers building client and server applications leveraging the Rainbow CPaaS capabilities (see https://hub.openrainbow.com)
- SIP devices are also supported in the context of the Rainbow Hub offer, in regions where it is available

The following picture provides the global overview of Rainbow from network perspective:



UDP	30000-44999	SRTP media	SIP devices	*.openrainbow.com
UDP	53	DNS	SIP devices	DNS server
UDP	123	NTP	SIP devices	pool.ntp.org

(a) details on FQDN and IP addresses of Rainbow servers are provided in section 5

(b) Google requires that if the network implements Network Address Translation (NAT) or Stateful Packet Inspection (SPI), a 30 minute or larger timeout is maintained for FCM connections over ports 5228-5230

3.3 High-Level Principles and Flows

All applications aim at providing the same level of services and features and interact with server-side components for signaling and media. The basic principles are provided in this section, and a detailed list of protocols/ports in the following one.

3.3.1 Signaling for WebRTC calls

For signaling, HTTPS/REST and Secured Web Sockets protocols are used:

- HTTPS (443) for all REST API communications and resources loading.
- Secure Web Sockets (WSS, 443) for all XMPP messages and notifications.

If a HTTP Proxy is configured, HTTP Proxy is used. In such case, HTTP Proxy must support Secured WebSocket (HTTP Upgrade to switch to wss protocol).

		Audio/video/desktop sharing media for collaboration		
TCP [d]	5228-5229-5230	Android push notification	Rainbow on pure wifi Android devices	Google FCM servers
TCP	443	Apple push notification	Rainbow on pure wifi ios devices	Apple APNS servers

(a) details on FQDN and IP addresses of Rainbow servers are provided in section 5

(b) the solution can fall back on TCP/443 if the infrastructure does not allow UDP (UDP remains highly recommended for best quality of service for multi-media flows)

(c) the NAT gateway implemented between the WebRTC Gateway and Rainbow must avoid too fast reuse of WAN ports. This can be achieved by implementing a 10mn timeout on NAted connection. See note of section 4.6.1 for details.

(d) Google requires that if the network implements Network Address Translation (NAT) or Stateful Packet Inspection (SPI), a 30 minute or larger timeout is maintained by firewalls for FCM connections over ports 5228-5230. See section 4.2

3.2.3 Rainbow Hub

The table below gives minimum requirements for deployment of the Rainbow Hub solution. The latter provides cloud telephony services and optionally advanced collaboration services.

Protocol	Destination Port	Main use	Source	Destination [a]
TCP	443	Signaling, APIs Messaging, filesharing	Rainbow applications	*.openrainbow.com openrainbow.com openrainbow.io
UDP	3478	Softphony Audio/video/desktop sharing media	Rainbow applications	*.openrainbow.com
TCP [b]	5228,5229,5230	Android push notif.	Rainbow on pure wifi Android devices	Google FCM servers
TCP	443	Apple push notif.	Rainbow on pure wifi ios devices	Apple APNS servers
TCP	5061	SIP	SIP devices	*.openrainbow.com
TCP	443	Config and APIs	SIP devices	*.openrainbow.com

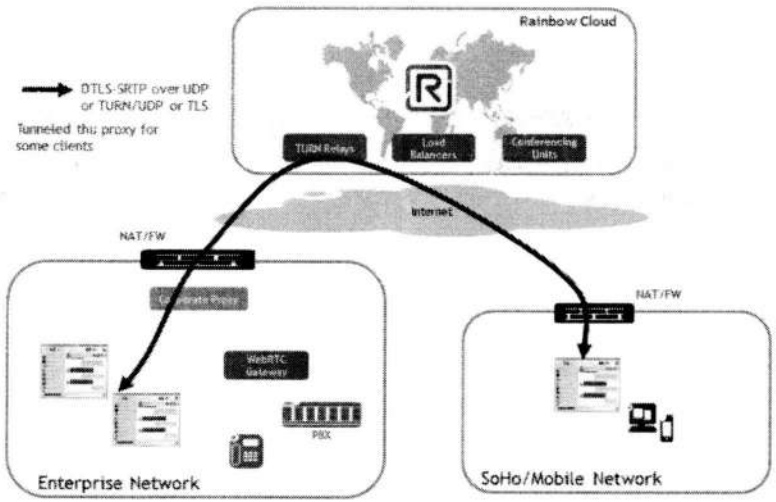
- Clients then check connectivity for candidates between both clients and select the most optimized working pair.

In case network conditions loss/change during an established communication, the network path for media is automatically renegotiated on-the-fly thru the above ICE mechanisms, allowing to keep communication active with only a small media interruption (no more than a few seconds max for device to change network connection and Rainbow WebRTC stack to perform re-negotiation). This typically happens in case of Wi-Fi/3G-4G handover for mobile devices, or network connectivity change on computer (wired to Wi-Fi connection).

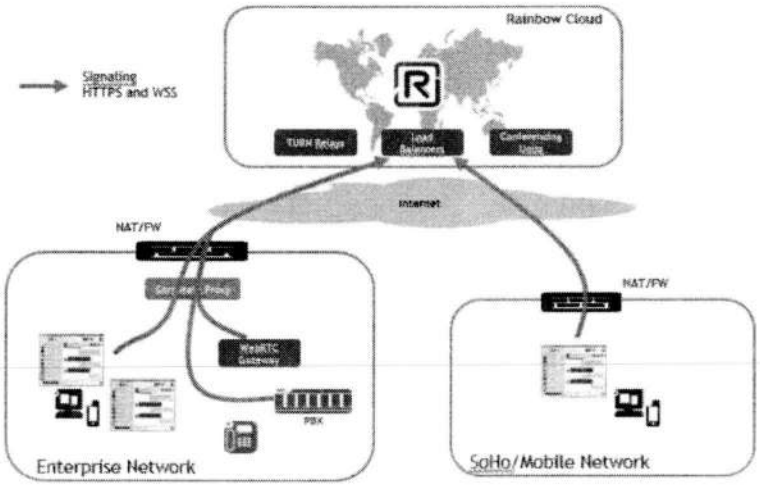
Example1: P2P WebRTC between local client (Enterprise network) and Remote client (external to the Enterprise network)

In such a case, a direct connection is not possible and the communication is generally achieved by leveraging a TURN server, acting as a cloud relay for routing media. It is reminded here that TURN relays are simple traffic redirectors, and have no access to the relayed media that remains encrypted end-to-end between peers.

As illustrated below, in case a proxy is used on the enterprise network, the connection to the TURN servers, and consequently the media, can be tunneled thru the proxy for some Rainbow clients (see details in section 0).



Note: to simplify figures, only one TURN server is illustrated. For a P2P communication, depending on geography and network performance, up to two TURN servers could be used to establish a communication (a different one for each client).



Full details on the involved ports are provided in the next sections.

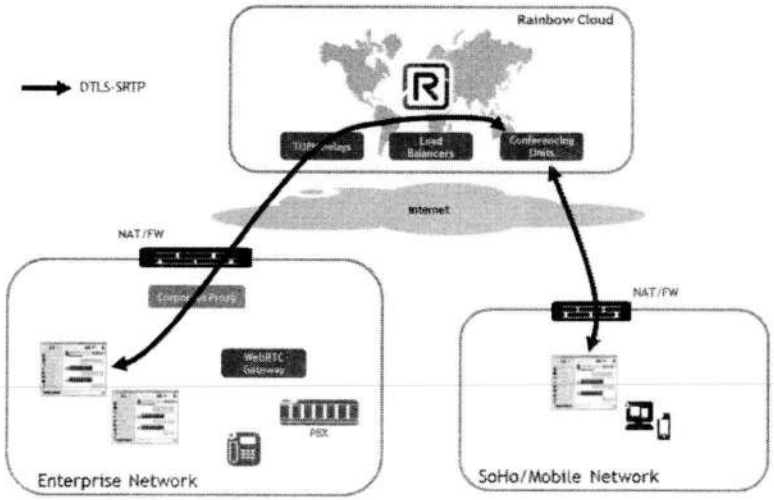
3.3.2 WebRTC/Media

Media communications between two clients, or between client and server-side conferencing components, use the WebRTC technology with DTLS-SRTP protocol for encrypting audio, video and desktop sharing media. The solution leverages ICE mechanisms and Rainbow TURN relays to achieve connectivity thru NAT/Firewalls.

ICE (Internet Connectivity Establishment) procedure and STUN/TURN protocols are used to dynamically determine how the media will be routed between two Rainbow clients.

Basically, when a WebRTC communication takes place, client proceeds to the following steps:

- Each client gathers candidates addresses.
  - A candidate is a transport address, combination of IP address and port for a particular transport protocol, allocated on local interface (for example wired Ethernet interface or WiFi interface for a PC), and on TURN cloud relay server that are necessary to allow cross network communications. The Rainbow infrastructure ensures TURN servers are located in all regions for providing world-wide coverage, however for optimizing the number of candidates for a WebRTC communication, Rainbow clients are automatically using only the nearest two Rainbow TURN servers, based on their IP geo-localization.
- The client exchanges candidates with the distant peer (other client or conferencing unit),



3.3.3 WebRTC for Hybrid Softphony calls

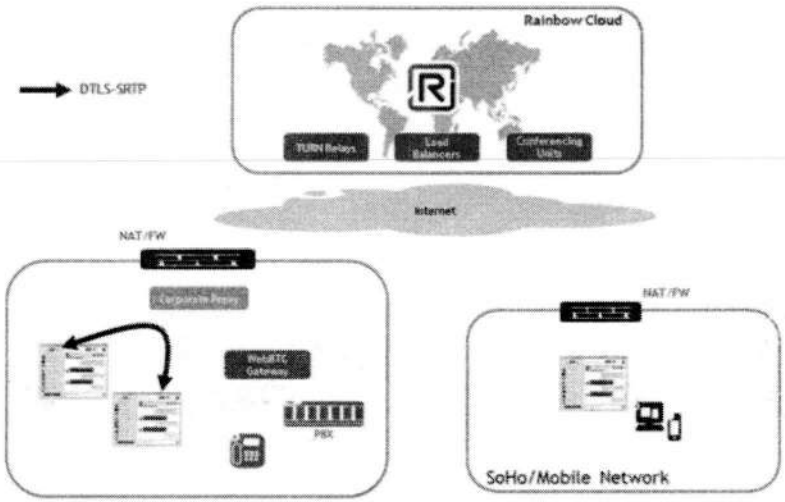
In hybrid mode, PBX telephony calls placed or taken with Rainbow clients also use the WebRTC technology and principles described in the above section, where one end of the WebRTC media call is the WebRTC Gateway. The latter acts as gateway between the Rainbow client used for the softphone call, WebRTC being used between Rainbow client and Gateway, whereas the gateway interfaces with the PBX in SIP and with PBX devices in RTP.

As for previous examples, the media path depends on whether the WebRTC Gateway and the Rainbow client are located on a same network and can therefore have a direct connection between each other. If this connection is possible, the call is direct between the WebRTC Gateway and the Rainbow application. If no direct connectivity exists, then the call is relayed thru a TURN server.

The two scenarios are depicted below.

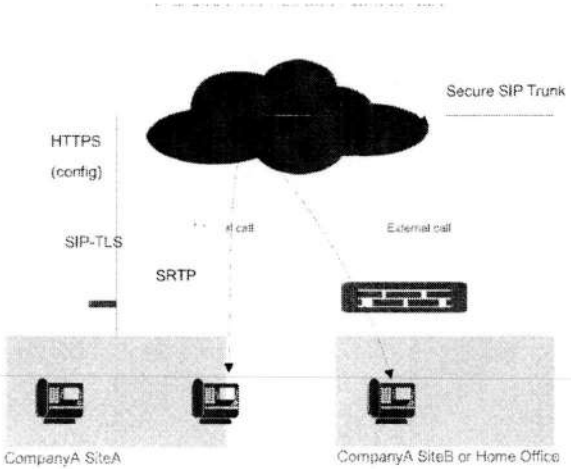
Example2: P2P WebRTC between two clients located on same LAN (Enterprise network)

In such a case, a direct connection is possible and the ICE negotiation results in clients choosing the direct path, as preferred path over the one going thru TURN.



Example3: Media with WebRTC Rainbow conference (Bubble)

When joining an Audio/Video Rainbow conference (bubble), clients connect to Rainbow cloud Conferencing Unit. Depending on the type of network infrastructure (Firewall/NAT type) on client side, clients either join the conferencing unit directly, or by getting relayed thru a TURN server, typically if UDP is not allowed directly between endpoints and the conferencing unit.



The configuration file contains the SIP parameters that then allow SIP devices to register to the platform through the nearest SIP entry point, and consequently establish the signaling link based on SIP-TLS. The SIP-TLS link is always to the initiative of the device, and maintained permanently with the Rainbow back-end thanks to keepalive traffic sent over the SIP-TLS connection.

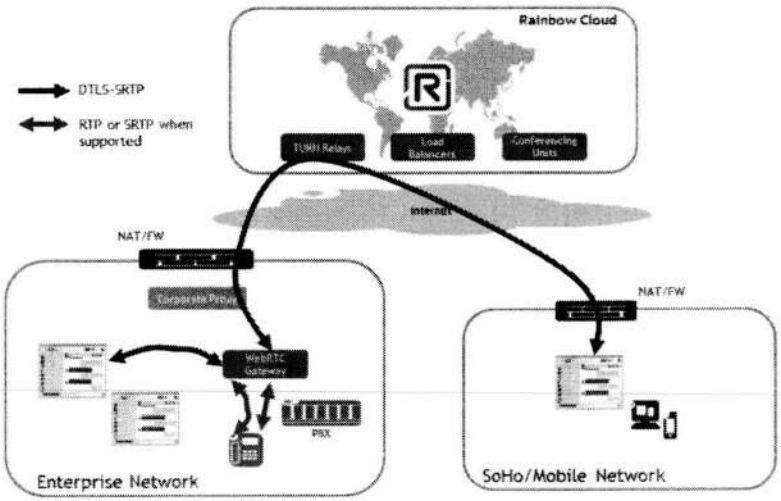
Calls are always established using SRTP protocol (RFC3711), relayed thru the Rainbow platform. The solution automatically adapts to NAT and uses the connection initiated by the device through the remote firewall/NAT component if any, to exchange media flows in both directions.

Call scenarios with Rainbow clients

Rainbow desktop/web and mobile clients can be used as softphone, to place and receive telephony calls to/from local or external extensions through the Rainbow Hub infrastructure.

Rainbow clients keep relying on WebRTC technology for these scenarios, and on the principles and protocols described in section 3.3.2.

When interacting with SIP devices or with an external extension through the SIP trunk, the mediation between WebRTC/DTLS-SRTP and SIP-TLS/SRTP is managed by the Rainbow infrastructure.



3.3.4 Rainbow Hub

Rainbow Hub is a full cloud telephony and UC offer, rendering services on SIP devices connected directly to Rainbow cloud infrastructure, as well as on Rainbow clients, and applications built on top on Rainbow APIs. Traffic to/from the public network is enabled thanks to partner-provided SIP trunks, connected on the Rainbow backend.

Telephony services come in addition to other UCaaS and CPaaS services which network flows are already described in previous sections.

Specific flows are the ones involving SIP endpoints, that rely on the following secure protocols:

- HTTPS for automated configuration retrieval and firmware updates, for devices which are fully managed by Rainbow
- SIP-TLS for signaling towards Rainbow SIP cloud entry points
- SRTP for media

All flows are initiated from the devices towards Rainbow, removing need to open any incoming port. All used protocols are compatible with NAT.

The main scenarios are illustrated hereafter.

Call scenarios with SIP devices

As depicted below, managed SIP devices automatically connect to Rainbow cloud to get their configuration and firmware updates from Rainbow, using HTTPS protocol. Phones are automatically recognized by Rainbow, after digital certificate and MAC address verification. Al HTTPS requests are outgoing from SIP devices to Rainbow.

169

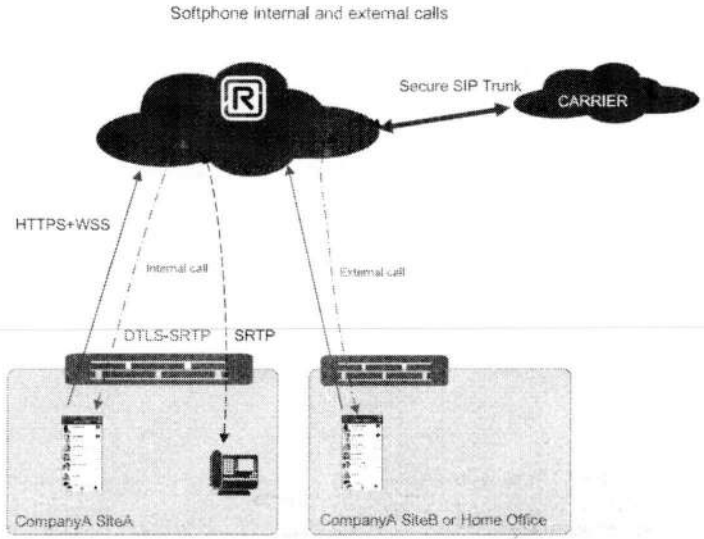
4 Detailed List of used Protocols and Ports

4.1 Rainbow Desktop and Web clients and Web SDK

Note that IP flows are always at the initiative of the clients, so no inbound firewalls rules from Internet to the enterprise network are needed.

The following connections take place between Rainbow client/Agent and Rainbow Cloud Services, possibly going thru a proxy if one is configured on the computer.

Protocols	Source	Destination	HTTP Proxy Compatibility
Signaling and APIs (mandatory)			
HTTPS (Resources and REST API. Apps updates)	**Rainbow client** OS dynamic port range (see 5.3.5)	**Rainbow servers,** TLS/443	**Yes**
Secure Web Sockets - WSS (XMPP)	**Rainbow client** OS dynamic port range	**Rainbow servers,** TLS/443	**Yes**
Pure WebRTC Audio/Video/ScreenSharing			
DTLS-SRTP for Peer-to-Peer WebRTC comm on same LAN (Rainbow clients have direct connectivity between each-other)	**Rainbow client** OS dynamic port range	**Peer Rainbow client** UDP OS dynamic port ranges	Not applicable (such flows remain on LAN)
DTLS-SRTP for Peer-to-Peer WebRTC comm thru Internet	**Rainbow client** OS dynamic port range	**Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443 TCP/80 (see note1) (see note3)	**Yes,** requesting proxy to connect to TURN servers via ports TLS/443 and TCP/80 (see note1&2)
DTLS-SRTP to Rainbow WebRTC Conference servers	**Rainbow client** OS dynamic port range	**Rainbow conference servers** UDP port range UDP/49152-65535 As fallback if outgoing	**Yes,** requesting proxy to connect to TURN servers via ports TLS/443 and TCP/80 (see note1&2)



		UDP range is not opened: **Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443 TCP/80 (see note1)	
Hybrid Softphony (on ALE OXE/OXO/OTEC or supported 3d party PBX)			
DTLS-SRTP for Softphone call when the app is on LAN and can reach the WebRTC Gateway	**Rainbow client** OS dynamic port range	**WebRTC Gateway** UDP 20000-29999	Not applicable (such flows remain on LAN)
DTLS-SRTP for Softphone call when the app is not on same LAN as WebRTC Gateway	**Rainbow client** OS dynamic port range	**Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443 TCP/80 (see note1) (see note3)	**Yes**, requesting proxy to connect to TURN servers via ports TLS/443 and TCP/80 (see note1&2)
Rainbow Hub Softphony			
DTLS-SRTP for Softphone call	**Rainbow client** OS dynamic port range	**Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443	**Yes**, requesting proxy to connect to TURN servers via ports TLS/443 and TCP/80 (see note1&2)

Note1: Firefox does not correctly support TURN-TLS thru proxy at present time, ie version 64 for this document edition. TCP-80 is offered as a workaround, and port 80 must therefore be opened in firewalls for outgoing traffic when Firefox is being used thru a proxy. It is reminded that the usage of port TCP-80 does not imply clear media traffic. This port is only used as transport channel to the TURN server, and the applicative flow conveyed over it is encrypted end-to-end with DTLS-SRTP

Note2: DPI compatibility. The connection between a browser and the TURN Server, using TCP-80 or TCP-443 ports, are not using HTTP protocol beyond the HTTP CONNECT allowing the proxy to open the tunnel, but STUN/TURN and DTLS-SRTP protocols. In case Deep Packet Inspection is applied on the customer network and expects to examine HTTP traffic, exception rules must be applied for traffic to Rainbow TURN IP addresses, so the DPI gear allows this legitimate Rainbow TURN connections without attempt for intermediate decryption neither HTTP inspection.

Note3: The firewall will actually see tentative traffic to other destinations/ports, but the above table only lists the minimum required ports for ensuring correct functional behavior with less possible opened rules. Indeed, ICE connectivity checks, as described in 3.3.2, test all possible combinations of IP/ports between the local client and the remote peer candidates. As each peer generally provides candidates with local address (LAN), public relayed address (exposed at a TURN Server), and reflexive address (corresponding to their Internet access gateway), STUN connectivity checks are exchanged between all possible pairs, some being between the WebRTC Gateway and any possible remote IP address and port, which would be enabled by opening a firewall rule towards <any>/<any> IP/port tuple. Only allowing traffic to the TURN server avoids opening such a wide rule. It results in part of the connectivity checks to fail (the ones targeted at the peer reflexive address for example) but ensures that a media path is always found via a rainbow TURN server.

thru Internet	range	UDP/3478 TLS/443 (note3)	the firewall, the app automatically falls back to mobile data network if such connectivity is available For WiFi-only mobile devices, the IS/IT must open UDP/3478 and/or TLS/443 to Rainbow Servers
DTLS-SRTP to Rainbow WebRTC Conference servers	**Rainbow client** OS dynamic port range	**Rainbow conference servers** UDP port range UDP/49152-65535 As fallback if outgoing UDP range is not opened: **Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443	
Hybrid Softphony (on ALE OXE/OXO/OTEC or supported 3d party PBX)			
DTLS-SRTP for WiFi Softphone call when the app is on LAN and can reach the WebRTC Gateway	**Rainbow client** OS dynamic port range	**WebRTC Gateway** UDP 20000-29999	Not applicable (such flows remain on LAN)
DTLS-SRTP for Softphone call when the app is not on LAN as WebRTC Gateway	**Rainbow client** OS dynamic port range	**Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443 (note3)	**No**, proxy not supported for media If ports are blocked on the firewall, the app automatically falls back to mobile data network if such connectivity is available For WiFi-only mobile devices, the IS/IT must open UDP/3478 and/or TLS/443 to Rainbow Servers
Rainbow Hub Softphony			
DTLS-SRTP for Softphone call	**Rainbow client** OS dynamic port range	**Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443	**No**, proxy not supported for media If ports are blocked on the firewall, the app automatically falls back to mobile data network if such connectivity is

172

4.2 Rainbow Android and iOS clients and associated SDKs

The flows involved with mobile clients are similar to the ones used by computer apps, at the exception of proxy compatibility for media, and of the push notification channel required for users to properly receive incoming events (IM, call) when the app is not in foreground.

Proxy settings are inherited from device network configuration.

Protocols	Source	Destination(s)	HTTP Proxy Compatibility
Signaling and APIs (mandatory)			
HTTPS **(Resources and REST API)**	**Rainbow client** OS dynamic port range (see 5.3.5)	**Rainbow servers,** TLS/443	**Yes**
Secure Web Sockets - WSS **(XMPP)**	**Rainbow client** OS dynamic port range	**Rainbow servers,** TLS/443	**Yes**
Apple Push Notification **(iOS App)**	**Rainbow device** OS dynamic port range	**APNS** TCP/443 (*)	**No** If the ports are not opened on the firewall, the app automatically falls back to mobile data network if such connectivity is available For WiFi-only mobile devices, the IS/IT must open firewall rules to allow direct outgoing traffic to Push Notification ports
Google FCM Push Notification **(Android app)**	**Rainbow device** OS Dynamic port range	**Google FCM servers** TCP/5228-5229-5230 (**) TCP/443	
Pure WebRTC Audio/Video/ScreenSharing			
DTLS-SRTP for Peer-to-Peer WebRTC comm on same LAN (Rainbow clients have direct connectivity between each-other)	**Rainbow client** OS dynamic port range	**Peer Rainbow client** UDP OS dynamic port ranges	Not applicable (such flows remain on LAN)
DTLS-SRTP for Peer-to-Peer WebRTC comm	**Rainbow client** OS dynamic port	**Rainbow TURN Servers** using several connectivity alternatives:	**No**, proxy not supported for media If ports are blocked on

Google FCM Push Notification **(Android app)**	**Rainbow device** OS Dynamic port range	**Google FCM servers** TCP/5228-5229-5230 (**)	**No** The IS/IT must open firewall rules to allow direct outgoing traffic to Push Notification ports
Pure WebRTC Audio/Video/ScreenSharing			
DTLS-SRTP for Peer-to-Peer WebRTC comm on same LAN (Rainbow clients have direct connectivity between each-other)	**Rainbow client** OS dynamic port range	**Peer Rainbow client** UDP OS dynamic port ranges	Not applicable (such flows remain on LAN)
DTLS-SRTP for Peer-to-Peer WebRTC comm thru Internet	**Rainbow client** OS dynamic port range	**Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443	**No**, proxy not supported for media The IS/IT must open UDP/3478 and/or TLS/443 to Rainbow Servers
DTLS-SRTP to Rainbow WebRTC Conference servers	**Rainbow client** OS dynamic port range	**Rainbow conference servers** UDP port range UDP/49152-65535 As fallback if outgoing UDP range is not opened: **Rainbow TURN Servers** using several connectivity alternatives: UDP/3478 TLS/443	

4.5 PBX Agents

PBX agents, embedded in ALE PBX or deployed as external component for third party PBX, require connecting to Rainbow Cloud to deliver hybrid telephony services. As for other Rainbow CPE components, all flows are initiated from PBX Agent to Rainbow cloud, avoiding opening any incoming firewall pinholes from Internet to the corporate network.

The following table details IP flows required for the agent to connect to Rainbow servers.

Protocols	Source	Destination(s)	HTTP Proxy Compatibility

173

			available For WiFi-only mobile devices, the IS/IT must open UDP/3478 and/or TLS/443 to Rainbow Servers

(*) reference: https://support.apple.com/en-ph/HT203609

(**) reference: https://firebase.google.com/docs/cloud-messaging/concept-options

Note the important requirement from Google for push notification delivery:

"If your network implements Network Address Translation (NAT) or Stateful Packet Inspection (SPI), implement a 30 minute or larger timeout for our connections over ports 5228-5230. This enables us [Google] to provide reliable connectivity while reducing the battery consumption of your users' mobile devices"

(note3): see note3 of 4.1

4.3 Rainbow Teams and Google Connectors

Teams and Google connectors rely on Rainbow Web SDK and allow leveraging Rainbow Hybrid and Cloud telephony capabilities from within Microsoft and Google software suites. The network flows involved are identical to the ones of the Rainbow desktop/web, please refer to section 4.1.

4.4 Rainbow Room

Rainbow rooms are Android clients and therefore rely on the same flows as Android smartphones applications.

Protocols	Source	Destination(s)	HTTP Proxy Compatibility
Signaling and APIs (mandatory)			
HTTPS **(Resources and REST API)**	**Rainbow client** OS dynamic port range (see 4.8)	**Rainbow servers,** TLS/443	**Yes**
Secure Web Sockets - WSS **(XMPP)**	**Rainbow client** OS dynamic port range	**Rainbow servers,** TLS/443	**Yes**

			cases**
DTLS-SRTP for Peer-to-Peer WebRTC comm thru Internet	**WebRTC Gw** UDP 20000-29999	**Rainbow TURN Servers** UDP/3478***	**Yes*** Requesting proxy to connect to TURN servers via port TCP/80 by default, when mpmproxy command is used. Use of TLS/443 is possible for specific cases**

* *the WebRTC Gateway supports HTTP proxy for media since version 1.71, by having the admin use the mpmproxy command so proxy is used instead of direct connection to TURN UDP/3478. Note that a direct connection to TURN servers, using UDP, remains the recommended way for Voice quality reasons, as it avoids TCP-related retransmissions if the network experiences packet loss. Connection via proxy requires the proxy to implement HTTP version 1.1*

** *Using TCP/80 is the default because the channel to the TURN only conveys DTLS-SRTP encrypted media. Therefore TCP/80 avoids double encryption which impacts performances and may affect QoS. Proxying to TURN servers on TLS/443 is supported as a workaround for proxies or policies that may not allow proxying to TCP/80, but impacts the number of simultaneous communications the component can support*

*** *The firewall will actually see tentative traffic to other destinations/ports, but the above table only lists the minimum required ports for ensuring correct functional behavior with less possible opened rules. Indeed, ICE connectivity checks, as described in 3.3.2, test all possible combinations of IP/ports between the local client and the remote peer candidates. As each peer generally provides candidates with local address (LAN), public relayed address (exposed at a TURN Server), and reflexive address (corresponding to their Internet access gateway). STUN connectivity checks are exchanged between all possible pairs, some being between the WebRTC Gateway and any possible remote IP address and port, which would be enabled by opening a firewall rule towards <any>/<any> IP/port tuple. Only allowing traffic to the TURN server avoids opening such a wide rule. It results in part of the connectivity checks to fail (the ones targeted at the peer reflexive address for example) but ensures that a media path is always found via a rainbow TURN server.*

Important : Concerning NAT configuration, the NAT gateway must be configured so the source port used at the WAN side is not reused too quickly for a subsequent call. This can be achieved either by implementing a static NAT/PAT logic (1 to 1 source port between WRG and NAT gateway) or by ensuring the port range of the NAT gateway is wide enough and with cyclic allocation, or that a TTL of at least 10 minutes is configured for traffic towards TURN servers UDP/3478.

4.6.2 WebRTC Gateway flows to PBX and local devices/clients

Besides these flows with the Rainbow ecosystem, the WebRTC Gateway communicates with the PBX ecosystem on the LAN. The flows are described hereafter in case firewalling is applied between WebRTC Gw and the LAN side.

Protocols	Source	Destination
SIP	**WebRTC Gw**	**PBX (physical IP address)**

Secure Web Sockets - WSS	**PBX Agent** PBX dynamic port range	**Rainbow servers,** TLS/443	**Yes**
DNS	**PBX Agent**	**DNS Server (*)** UDP/53	**No**

(*) The DNS server, generally located on corporate network, is required to resolve Rainbow server names.

4.6 WebRTC gateway

In hybrid softphony configurations with ALE PBX or supported 3d party PBX, the WebRTC Gateway acts as a bridge enabling media communications between Rainbow WebRTC clients and telephony extensions reached thru a PBX. It is deployed on the same network as the PBX.

Important: The configuration of a DNS server in the WebRTC Gateway is mandatory, even if only IP addresses are used. This limitation is linked to some internal components that will perform a reverse DNS query before the usage of the proxy.

4.6.1 WebRTC gateway to Rainbow Cloud

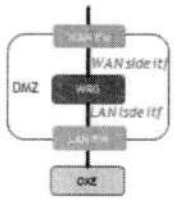
The following table details the flows involved between the WebRTC Gateway and other Rainbow components on Cloud side

Protocols	Source	Destination	HTTP Proxy Compatibility
HTTPS (Resources and REST API)	**WebRTC Gw** OS dynamic port range (see 4.8)	**Rainbow servers,** TLS/443	**Yes**
Secure Web Sockets - WSS (XMPP)	**WebRTC Gw** OS dynamic port range	**Rainbow servers,** TLS/443	**Yes**
ICE/TURN(s) Media Connectivity Checks	**WebRTC Gw** UDP 20000-29999	**Rainbow TURN Servers** UDP/3478***	**Yes*** Requesting proxy to connect to TURN servers via port TCP/80 by default, when mpmproxy command is used. Use of TLS/443 is possible for specific

4.6.3 WebRTC gateway in the DMZ

The WebRTC Gateway supports being deployed in a DMZ. It is however not a security border element, and must therefore be protected by firewalls, and must not be directly exposed on the internet.

To allow segmenting the flows from WAN and LAN side on different subnets within the DMZ, a second interface can be optionally activated on the WebRTC Gateway.



Should the WebRTC Gateway be deployed in a DMZ, make sure the following requirements are addressed:

- NAT is not supported between the WebRTC Gateway and the PBX or devices, so no NAT between the DMZ and the LAN
- Internal and external firewall must allow all necessary traffic as detailed in the above sections, more specifically
  - The WAN side firewall must enable all outgoing traffic as described in 4.6.1
  - The LAN side firewall must enable all flows detailed in 4.6.2

4.7 Rainbow Hub ALE SIP devices

This section lists the flows required for SIP devices to connect to Rainbow. It is only relevant in the context of the Rainbow Hub Offer.

Note: ALE SIP terminals do not support crossing HTTP proxy currently

Protocols	Source	Destination
SIP over TLS	**Desk phones** TCP/5061	**Rainbow Cloud PBX** TCP/5061
HTTPS	**Desk phones** OS Dynamic range	**Rainbow Device Discovery Service** TCP/443
SRTP Media	**Desk phones** UDP 30000-40000	**Rainbow Cloud PBX** UDP 30000 / 44999

	UDP/5060	UDP/5060
SIP	**PBX (physical IP Address)** UDP/5060	**WebRTC Gw** UDP/5060
RTP Media	**WebRTC Gw** UDP 30000-40000	**PBX Gateway and SIP Trunk SBC** UDP port range (*)
RTP Media	**PBX Gateway and SIP Trunk SBC** UDP port range (*)	**WebRTC Gw** UDP 30000-40000
RTP Media	**WebRTC Gw** UDP 30000-40000	**IP Phones** UDP port range (*)
RTP Media	**IP Phones** UDP port range (*)	**WebRTC Gw** UDP 30000-40000
WebRTC Media	**WebRTC Gw** UDP 20000-29999	**LAN side Rainbow clients** UDP OS dynamic port range (*)
WebRTC Media	**LAN side Rainbow clients** UDP OS dynamic port range (*)	**WebRTC Gw** UDP 20000-29999
DNS (**)	**WebRTC Gw** UDP/1024-65535	**DNS server** UDP/53
NTP	**WebRTC Gw** UDP/123	**NTP server** UDP/123
SSH *If enabled*	**SSH client**	**WebRTC Gw** TCP/22

(*) please refer to IP Flows PBX documentation on BPWS, for precisions on gateway and devices port ranges.

(**) The configuration of a DNS server in the WebRTC Gateway is mandatory to resolve Rainbow servers FQDN, even in configurations relying on a proxy. This constraint is linked to some internal components that will perform a reverse DNS query before the usage of the proxy.

Used by	Purpose	Domains
Rainbow Clients	Resources (website, images, client package, Agent package, ...)	web.openrainbow.com cdn.openrainbow.com meet.openrainbow.com webinar.openrainbow.com
Rainbow Clients/SDK	REST API	openrainbow.com
Rainbow Clients/SDK	XMPP over Secured WebSockets	openrainbow.com
Teams/Google and ITSM/CRM connectors	Resources and APIs *(in addition to all domains used by Rainbow clients/SDK)*	*.openrainbow.io (wildcard)
Developper Hub	Documentations and SDKs	hub.openrainbow.com
Rainbow Clients/SDK	STUN/TURN	turn-*.openrainbow.com (wildcard) turn-bhs1.openrainbow.com (Canada) turn-cap1.openrainbow.com (South Africa) turn-bhr1.openrainbow.com (Bahrain) turn-che1.openrainbow.com (India) turn-dal1.openrainbow.com (US West) turn-hkg1.openrainbow.com (Hong-Kong) turn-lim1.openrainbow.com (Germany) turn-lim2.openrainbow.com (Germany) turn-rbx1.openrainbow.com (France) turn-rbx2.openrainbow.com (France) turn-sao1.openrainbow.com (Brazil) turn-sao2.openrainbow.com (Brazil) turn-seo1.openrainbow.com (South Korea) turn-sgp1.openrainbow.com (Singapore) turn-sjc1.openrainbow.com (US West) turn-syd1.openrainbow.com (Australia) turn-tok1.openrainbow.com (Japan) turn-vin1.openrainbow.com (US East) turn-dli2.myopenrainbow.cn.com (China)

DNS	**Desk phones** OS Dynamic range	**DNS server** UDP/53
NTP	**Desk phones** OS Dynamic range	**NTP server pool.ntp.org** UDP/123
SSH *If enabled*	**SSH client**	**Desk phones** TCP/22
HTTPS	**HTTPS client**	**Desk phones** **TCP / 443**

4.8 OS Dynamic port range

As complement to the info provided in the previous sections, the table below reminds the current default dynamic/ephemeral ports ranges used by the different operating systems Rainbow clients can run on. These ports are allocated by the OS and Rainbow apps have no control over this selection.

Supported Platforms	Dynamic Port Range (UDP and TCP)
Windows	49152-65535
MacOS	49152-65535
iOS	49152-65535
Android (>=7)	37000-50000
Linux WebRTC Gw	32768-60999

5 Rainbow Domains and IP addresses

This section lists the domains and IP addresses used for the Rainbow generic worldwide service.

For specific cases involving Rainbow Edge deployments, the principles described in the first part of the document apply, but domains and IP might differ. Please contact support if domains information is required for a specific Rainbow Edge.

To simply your firewall configuration, please consider allowing all subdomains of openrainbow.com and create a rule allowing any connection to *.openrainbow.com (wildcard). As alternative, you'll find below the current list of services and domains.

176

Used by	Purpose	Domains
Rainbow Clients/SDK	WebRTC conferences (for reverse DNS only)	rtc-*.openrainbow.com (wildcard) rtc-bhs1.openrainbow.com rtc-cap1.openrainbow.com rtc-bhr1,openrainbow.com rtc-gra2.openrainbow.com rtc-gra3.openrainbow.com rtc-gra4.openrainbow.com rtc-lim1.openrainbow.com rtc-lim2.openrainbow.com rtc-lim3.openrainbow.com rtc-rbx5.openrainbow.com rtc-rbx6.openrainbow.com rtc-rbx7.openrainbow.com rtc-sao1.openrainbow.com rtc-sao2.openrainbow.com rtc-sao3.openrainbow.com rtc-sgp1.openrainbow.com rtc-syd1.openrainbow.com rtc-vin1.openrainbow.com
Rainbow Clients/SDK	File sharing	files-*.openrainbow.com (wildcard) files-bhs.openrainbow.com files-lim.openrainbow.com files-sao.openrainbow.com files-sbg.openrainbow.com files-sgp.openrainbow.com files-syd.openrainbow.com files-us.openrainbow.com
PBX agent	PBX connection to Rainbow	agent.openrainbow.com
WebRTC GW	PBX media connection to Rainbow	As for Rainbow clients
Node Cli and SDKs in development mode	Sandbox connections for applications development tests	sandbox.openrainbow.com web-sandbox.openrainbow.com
Mail Server	For mails sent from Rainbow	smtp.openrainbow.com mail.openrainbow.com ms-*.openrainbow.com (wildcard) ms-sbg-2.openrainbow.com ms-bhs-2.openrainbow.com
SIP Desk phone for Rainbow Hub	Device discovery service used for firmware update, provisioning	rdd.openrainbow.com
SIP Desk phone for Rainbow Hub	Signaling and media to establish calls	*.eu1.sip.openrainbow.com (wildcard)

Nota: It is highly recommended that customers always use FQDNs, Rainbow servers IP addresses being subject to change. In the unfortunate event that using or whitelisting DNS entries is not an option, the table below references all public IP addresses used by the various Rainbow services. Please keep in mind that this map is subject to change and can be updated at any time without any further notice. Also keep in mind that due to the multiple high-availability and failover mechanisms in place, both at DNS and application levels, it is mandatory to whitelist all the IP addresses aforementioned, including those in regions and geographies that might not be explicitly those intended by end customer.

171

		169.56.128.9 169.56.36.238
	Oceania	139.99.148.135 139.99.161.35 139.99.177.193 139.99.212.212 139.99.212.213 139.99.212.214
TURN Media Relays	North America / US West	169.44.201.11
	North America / US Central	169.46.173.182
	North America / Canada	149.56.18.31
	South America / Brazil	169.57.174.104
	Europe / France	5.135.139.27 87.98.130.28
	Europe / Germany	217.182.197.194
	Asia / India	169.38.94.242
	Asia / Singapore	139.99.120.111
	Asia / Hong-Kong	169.56.128.10
	Asia / South-Korea	169.56.161.6
	Asia / China	42.202.135.13
	Asia / Japan	169.56.36.231
	Oceania / Australia	139.99.148.99
	Africa / South Africa	13.244.169.230
	Middle East / Bahrain	15.184.158.216
Conferencing Media Servers	North America / Canada	144.217.75.16
	South America / Brazil	169.57.174.106 169.57.207.29 169.57.207.3
	Europe / France	51.178.179.102 51.178.179.103 51.178.179.105 51.178.178.88 51.178.89.220 51.178.89.227
	Europe / Germany	51.89.99.90
	Asia / Singapore	139.99.122.114

Misc services *Those IPs can be dynamically associated to any below services, eg: load balancers, media relay, and decreases the number of changes needed on customer firewalls when Rainbow infrastructure changes*	North America / Canada	54.39.227.80/28
	North America / US	135.148.197.0/26
	South America / Brazil	
	Europe / France	5.135.82.192/28 51.75.103.64/27 51.178.224.224/27
	Europe / Germany	51.68.163.112/28 5.135.97.96/28
	Asia / Singapore	46.105.162.176/28
	Asia / China	
	Oceania / Australia	
Main Load Balancers	North America	142.4.216.72 167.114.175.31 167.114.135.97 149.56.179.10 144.217.123.252 169.44.201.2 144.217.133.89
	South America	169.57.207.27
	Europe	79.137.65.42 54.36.121.125 178.32.173.187 178.33.89.143 51.254.93.113 217.182.178.97 54.38.162.128 54.38.162.129 54.38.162.130 176.31.24.80 176.31.24.81 176.31.24.82
	Germany	54.36.108.169 51.38.111.143 51.89.55.153
	Asia	139.99.122.102 139.99.122.99 139.99.2.105 139.99.4.245 139.99.4.244 139.99.83.81 139.99.83.82 169.38.94.246

Peer to peer (P2P) WebRTC communications video resolution is 720p.

For Rainbow video conferences, Rainbow clients allows users to decide the way they want to see other participants video, ending up with different possible views:

- Active talker only: 1 high resolution 720p video displayed (if bandwidth permits). If screensharing is done in parallel, the active talker video is displayed in lower resolution
- Active talker with additional thumbnails: 1 high resolution 720p video (if bandwidth permits), and 180p videos for thumbnails[1]. If screensharing is done in parallel, the active talker video is also displayed in lower resolution. Web/Desktop application supports up to 5 thumbnails, 7 for Rainbow Room. This mode is not supported on mobile/tablet apps.
- Grid view with up to 12 videos for Web/Desktop or Room, and up to 6 for mobile applications): lower resolution (360p or 180p)[1] video streams (depending on network conditions)

The logic to manage different video resolutions relies on a simulcast technique. In upstream direction, depending on the available bandwidth and on server-side instructions, clients send up to 3 different video streams in different resolutions, enabling remote applications to subscribe to the most appropriate and optimized stream according to the selected view (active talker full screen, thumbnails or grid). Sending simulcast streams is currently only supported by Web/Desktop application, but all applications implement the selection of the appropriate stream on receiver end.

The following table provides maximum bandwidth requirement per media, from the perspective of a Rainbow application. Note that Rainbow sets an upper limit to the bandwidth consumed for video in 720p, 360p and 180p to respectively 800 kbps, 300 kbps and 100 kbps.

Media Type	Maximal Bandwidth	Average Bandwidth	Lowest Bandwidth	Comment
Audio (bi-directional)	100 kbps	40kbps	15kbps	
Screen Sharing (upstream for person who shares, downstream for others)	1.5 Mbps (720p)			Depends on screen motion figures here are max
Video p2p (bi-directional assuming the two person show their video)	P2P all Clients: 800 Kbps (720p)			actual bandwidth depends on network conditions, figures here are max
Video Conference	**Active talker-only view**: 800 Kbps (720p) **Act talk + thumbnails**: 800Kbps (720p) + N*100kbps (180p)[1]			actual bandwidth depends on network

	Asia / China	42.202.135.11 [redacted]
	Oceania / Australia	139.99.247.11
	Africa / South Africa	13.244.170.205
	Middle East / Bahrain	15.184.244.239
Mail	North America / Canada	54.39.227.85
	Europe / France	51.178.224.244
Cloud PBX (Rainbow Hub)	Europe / Germany	5.135.97.100
Device discovery service (Rainbow Hub SIP devices)	Europe / France	51.254.93.113 217.182.178.97 51.89.55.153
	Oceania / Australia	139.99.177.193
	Asia / Singapore	139.99.2.105 139.99.83.81
	North America / Canada	67.114.135.97 144.217.133.89
Connectors endpoints	World Wide	51.68.33.216 51.77.152.185 141.94.145.96/28

6 Bandwidth requirement

6.1 WebRTC for Rainbow peer-to-peer calls and multiparty conferences

Rainbow WebRTC communication currently rely on the following codecs:

WebRTC P2P:

- OPUS for audio
- VP8 or H.264 for Video and Screen Sharing

WebRTC Conference:

- OPUS for audio
- VP8 for Video and Screen Sharing

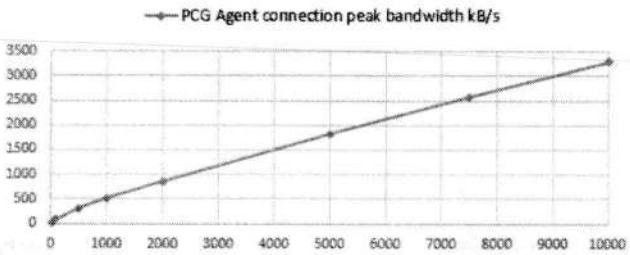
These WebRTC codecs are able to dynamically throttle both their resolution and bitrates, depending on network performance observed.

Connection to Rainbow Cloud

involving phonebook synchronization, as well as CTI monitoring initiation and phone state synchronization. This exchange takes place when the PBX Agent is started as well as when reconnecting following a broken connection due to an issue along the path.

The connection incurs a substantial burst of messages lasting anywhere from less than 1 second to 10 seconds depending on the number of PBX subscribers subject to Rainbow monitoring, whose rate is characterized in the following table:

# subscribers	20	100	500	1000	2000	5000	7500	10000
Connection Peak bandwidth kB/s	26	80	304	510	850	1818	2696	3294



Telephony events

Once connected, CSTA telephony events flowing in both directions in 1pcc or 3pcc contexts. The level of traffic here is directly proportional to call activity initiated on PBX side from endpoints or external inbound calls, or initiated from a Rainbow client in 3pcc mode. As such, this bandwidth is much lower than connection bursts, characterized as a function of the overall number of calls per second in busy hour rather than number of subscribers alone.

Calls / second	2	5	8	10	12
BHCA	7200	18000	28800	36000	43200
Bandwidth kB/s	3.5	9	14.4	18	21.7

180

Downstream direction	*(max N = 5 for web/desk, 7 for Room, N/A mobiles)* **Grid view:** 12 * 100 kbps (180p)(1)	conditions, figures here are max
Video Conference **Upstream direction**	Video upstream for Web/Desktop: 1.2 Mbps (720p+360p+180p) Video upstream for Mobile/Room: 800 Kbps (720p)(2) Sharing upstream: 1.5Mbps (720p)	actual bandwidth depends on network conditions, figures here are max

(1) if video is originated from an app that does not support simulcast, max video thumbnail is 720p rather than 180p

(2) to allow users to limit the used bandwidth on mobile devices where data plans are expensive, a parameter can be set to limit the video bandwidth (480p instead of 720p for upstream video, and downstream video throttled to 500 kbps)

6.2 Hybrid softphony calls

Business calls made or taken from CPE PBX and through the WebRTC gateway use G711 or G722 codecs for audio.

These codecs run at 64 kbps rate, which with addition of UDP and IP headers leads to 87.5kps.

It is reminded that real-time voice media is sensitive to the network quality, and that a good quality communication with G711 requires:

- One-way latency to be maximum 150ms
- Jitter to be maximum 30ms
- Packet loss to be maximum 1%

6.3 Rainbow Hub Softphony calls

Telephony calls placed or received with the Rainbow application to a SIP device or to PSTN, currently use G711 for media.

This codec runs at 64 kbps rate, leading to 87.5 kbps with UDP and IP headers.

It is reminded that real-time voice media is sensitive to the network quality, and that a good quality communication with G711 requires:

- One-way latency to be maximum 150ms
- Jitter to be maximum 30ms
- Packet loss to be maximum 1%

6.4 PBX Agent traffic

The PBX Agent acts as a CTI gateway between a local CPE PBX and the Rainbow Cloud, handling the following exchanges:

proxy for signaling, but media has to be enabled directly or by fallback on mobile data network (see chapter 4.2).

In case Deep Packet Inspection is implemented by proxy/firewall, some exceptions have to be configured for Rainbow, according to the Note of 4.1:

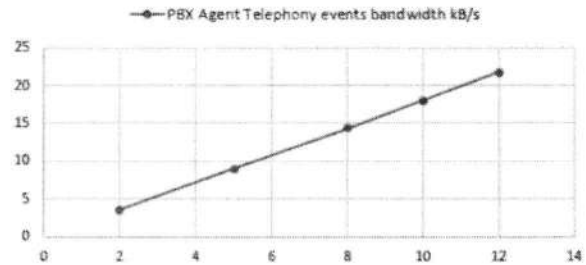
> *The connection between Rainbow clients or WebRTC Gateway and the TURN Servers, using TCP-80 or TCP-443 ports, are not using HTTP protocol beyond the HTTP CONNECT allowing the proxy to open the tunnel, but STUN/TURN and DTLS-SRTP protocols.*
>
> *In case Deep Packet Inspection is applied on the customer network and expects to examine HTTP traffic, exception rules must be applied for traffic to Rainbow TURN Servers, so the DPI policy allows this legitimate Rainbow TURN connections without attempt for intermediate decryption neither HTTP inspection.*

DPI exception can be applied on *.openrainbow.com. Note however that the WebRTC Gateway requires version 1.75 to send TURN FQDNs rather than IP addresses, in HTTP CONNECT. WRG must therefore be at minimum in version 1.75 for complying with DPI that only accept configuring exceptions based on FQDNs.

If must also be verified that the proxy is properly dimensioned, so it supports the number of simultaneous ports inferred by Rainbow usage:

- For signaling and APIs, each Rainbow client uses a permanent WSS towards Rainbow servers, and can perform parallel HTTPS requests for resources and APIs calls
- In addition to this, each WebRTC call via the proxy (ie involving a remote user) consumes additional ports for audio and video and sharing (one each in conference). Calls can be generated from Rainbow clients, and from the WebRTC gateway (possibly several hundred of simultaneous audio calls, refer to WebRTC Gateway capacity in TBE067 available on business partner web site)

Note finally that HTTP version 1.1 must be supported and used by the proxy, typically for the WebRTC Gateway to properly allow connecting to TURN server when a proxy is used.



Notes:

- The figures above are given in kilobytes per second, not kbps.
- The peak bandwidth is based on measurements conducted in real conditions from an enterprise site benefiting from an enterprise-grade WAN connection to the Rainbow Cloud with low latency, high bandwidth capacity. Actual WAN connections and/or local concurrent traffic may restrict the bandwidth available to the PBX Agent connection without consequence except for a longer time to connect.
- The peak bandwidth indicated here only accounts for the burst mostly induced by the phonebook synchronization. This burst is followed by a lower rate of CSTA exchanges to initiate the monitoring of devices, which for large PBXs can take several minutes for the connection to be fully operationnal.
- The simultaneous connection or reconnection of several PBX Agents cumulates the overall bandwidth requirements indicated here, possibly up to the common link capacity. If only one or some PBX Agents are to reconnect at the same time while others remain connected, the peak bandwidth requirement must be cumulated with the current telephony events traffic generated by already connected PBX Agents.
- The figures may be linearly interpolated to the actual number of subscribers.

7 Configuration of border elements in enterprise

7.1 DNS, Firewall, Proxy configuration

To allow Rainbow to operate properly, border elements like DNS, HTTP Proxy or Firewall must be configured to allow resolving accessing domains and protocols listed in the table of chapter 0 and 5.

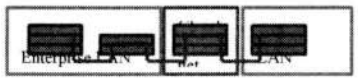
7.2 HTTP Proxy and DPI

If an HTTP Proxy is configured on the device where Rainbow applications are running, Rainbow Web and Desktop clients always rely on this HTTP Proxy to reach Rainbow cloud services (for all protocols used, including HTTPS/REST, XMPP over Secured Web Sockets and TURN). Mobile application use the

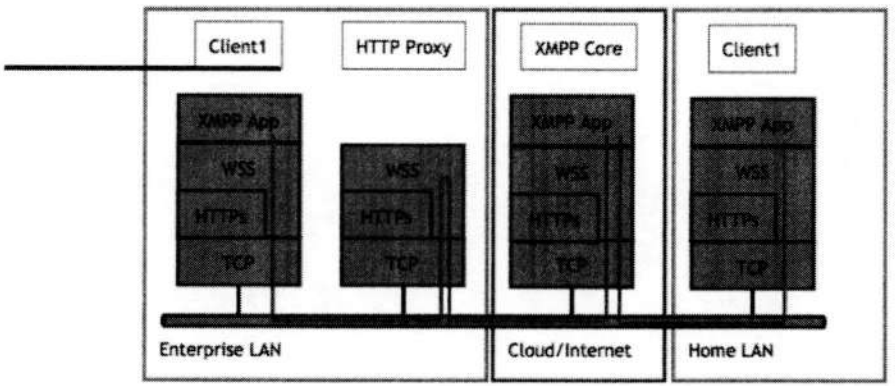
8 Annexes: Detailed call-flow of HTTPS/REST, XMPP and ICE connections

The following figures illustrate a case where Rainbow Client1 make an Audio/Video call to Rainbow Client2. Rainbow Client1 is in an enterprise environment with NAT/FW and HTTP Proxy border elements. Rainbow Client2 is in a Home network with simple NAT/FW as border element (home router/box).

Network layers (Rest API):

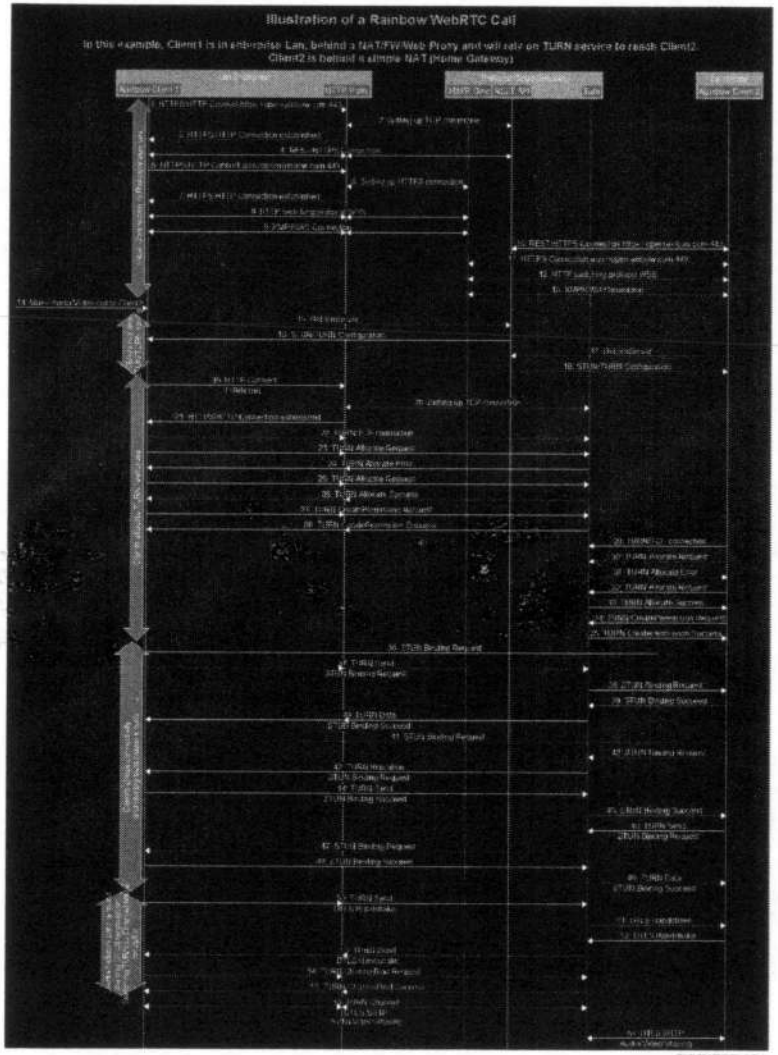


Network layers (XMPP):

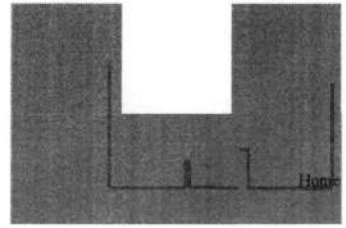


HTTPs is used to setup WSS protocol (RFC6455)

Call Flow:



Network layers (Media):



183

- Steps 1-9: Client1, behind HTTP Proxy, establish HTTPs sockets and Secured Web Sockets (for XMPP) through the HTTP Proxy.
- Steps 10-13: Client2, behind simple NAT, establish regular HTTPs sockets and Secured Web Sockets (for XMPP) directly to Rainbow Cloud Services.
- Step 14: Client1 make an Audio/Video call to Client2
- Steps 15-18: Client1 and Client2 retrieves ICE configuration (list of TURN servers)
- Steps 19-28: Client1 allocates TURN resources (through HTTP Proxy)
- Steps 29-35: Client2 allocates TURN resources (direct connection to TURN)
- Steps 36-49: Client1 and Client2 perform STUN connectivity check for various options (in this example, we illustrate the case where direct STUN connectivity check would failed)
- Steps 50-53: Client1 and Client2 have found a network path through the TURN server. They start to initiate the DTLS-SRTP handshake.
- Steps 54-55: Client1 ask TURN to switch to Channel mode to optimize network bandwidth (reduce TURN header overhead).
- Steps 56-57: DTLS-SRTP is established, Audio/Video media starts to flow between Client1 and Client2

End of Document

181