Unify OpenScape Voice

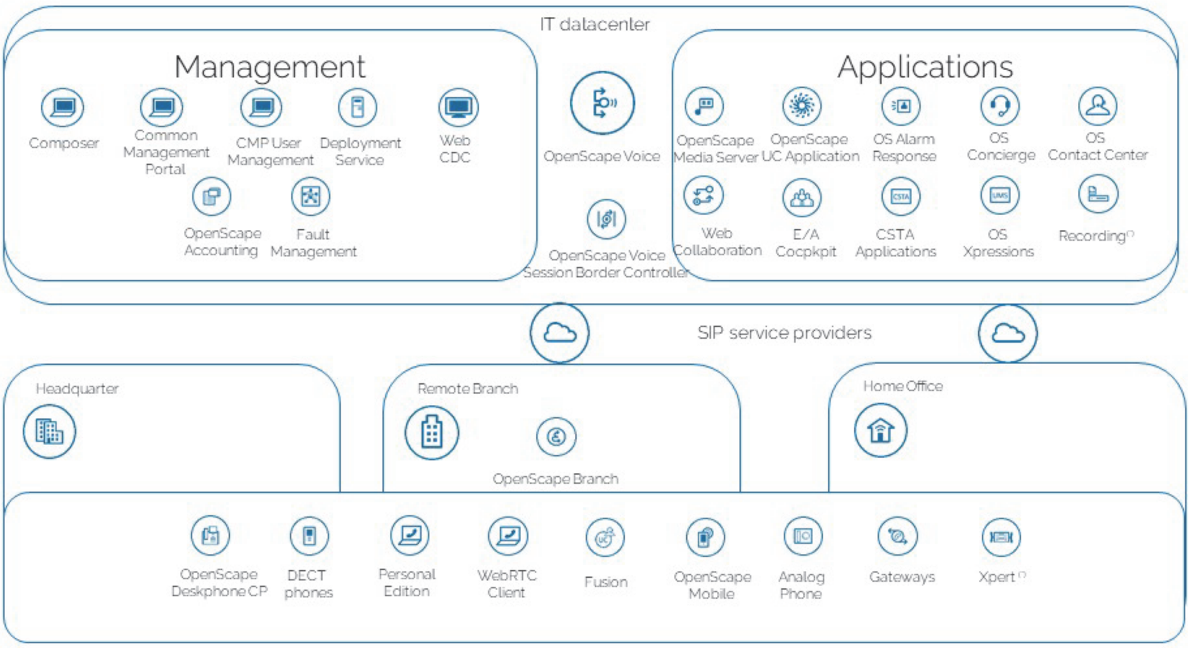
Atos Unify OpenScape Voice V10

Start with the right platform.
The leading software-based voice communications system

OpenScape Voice is a native SIP-based real-time Voice over IP system scalable up to 100,000 users per system and a virtually unlimited number of users when OpenScape Voice systems are networked. It provides a complete and feature-rich set of business class features and perfectly fits into data center installations running as a virtualized appliance on VMware hypervisors. Alternatively, it runs on highly reliable, redundant and fault-tolerant hardware.

OpenScape Voice can be deployed on premise or in data centers as Private Cloud or as multi tenant capable Hosted/Public Cloud solution.

OpenScape Voice is a carrier-grade enterprise voice solution meaning 99.999% reliability – that translates to less than 5 1/2 minutes of downtime per year! The server nodes are designed so that if one fails, the other server node can support 100% of the call load. The server nodes can operate with 100% call failover support even when they are geographically separated, greatly reducing the costs, and the amount of time implementing a disaster recovery strategy. And remote offices can be protected with an OpenScape Branch solution – a survivable branch office solution for OpenScape Voice. OpenScape Branch not only offers survivability, but it includes a media server, firewall, Session Border Controller, and integrated PSTN gateway, all in a single appliance form factor. The value of OpenScape Branch goes beyond survivability, its activity contributes to lower the overall deployment, bandwidth and service costs.



Third party

Comprehensive Unified Communications

OpenScape Voice is always part of a solution landscape. The most basic solution includes:

- OpenScape Voice as a SIP-based Voice over IP software application
- OpenScape Media Server for tones and announcements
- OpenScape Branch 550 and OpenScape Branch 550HA
- OpenScape Session Border Controller (SBC)
- OpenScape Desk Phone CP SIP phone family
- OpenScape Personal Edition (Soft client)
- OpenScape Common Management Platform (CMP) with OpenScape User Management
- OpenScape Deployment Service (Devices Management and User Mobility)
- OpenScape Composer

For advanced scenarios, Unified Communication applications are added.

Deployment scenarios

OpenScape Voice is designed to cover multiple customers and target market deployment scenarios. The key deployment scenarios are:

OpenScape Exchange

OpenScape Exchange is an overlay solution for multi-vendor networks, where there is TDM legacy, or converged IP systems. It allows for centralized deployment of Unified Communications services. In the overlay deployment, OpenScape Voice acts as a SIP-based central routing and administration solution for multi-site, multi-vendor networks, allowing customers a "migrate at your own pace" solution.

Public cloud / Hosted edition

OpenScape Voice is the cornerstone application for public cloud / hosted edition solutions. It supports multi-tenancy (up to 6,000 business groups) allowing service providers to "build their own cloud".

Private cloud

For large enterprise customers (1,000 to 100,000 users) with multi-site locations that span over a region or the globe, OpenScape Voice can deploy as a private cloud solution. The key characteristic of a private cloud is centralized deployment of voice (and UC) service from the customer's data center.

Configurations

OpenScape Voice Integrated Simplex

This configuration consists of a system that provides the medium-sized voice solution (with or without UC) in a single server. The OpenScape Voice and UC applications are deployed as a single node platform; as such there is no carrier-grade reliability due to the lack of redundancy. Additionally, the following deployment highlights provide the ability to run on the same physical platform:

- OpenScape Voice application
- OpenScape Voice Assistant
- OpenScape Media Server
- OpenScape Common Management Platform (CMP)
- OpenScape Deployment Service
- OpenScape UC

This model represents an offering that would be of interest to a customer that wants a medium sized VoIP business solution (up to 5,000 users) at a low cost, and therefore is willing to accept some risk of downtime (due to no redundancy). This is also a configuration that is prevalent in the "try-and-buy" program.

OpenScape Voice Duplex

This deployment model illustrates how the OpenScape Voice can be operated as a more robust and scalable duplex system. It provides carrier-grade reliability by running two platforms in a redundant two-node cluster that executes in an active-active mode. Should one of the nodes fail, then the remaining partner node would assume the call load of the failed partner (and would handle 100% of the call traffic) and would continue to provide uninterrupted call processing. No calls would be dropped due to the failover from duplex to simplex operation, or when the system reestablishes duplex operation. The duplex mode also allows for the possibility of maintaining call processing operation while an OpenScape Voice upgrade is performed.

Currently, a mix of physical nodes and virtual nodes is not supported. A cluster of 2 physical nodes or a cluster of 2 virtual nodes are the only scenarios supported.

This model is appropriate for larger customers (up to 100,000 users) as well as for customers that want carrier-grade reliability.

- Multiple instances of the OpenScape Deployment Service may be deployed to scale with the number of users. Running the OpenScape Deployment Service upon the same platform as the CMP is only recommended in very small deployments.
- A multi-node configuration for OpenScape Deployment Service is also supported. This allows an installation of two to four OpenScape Deployment Service servers to appear as a single computer to clients.
- The OpenScape Media Server scales (up to as many as 3,000) to meet the increased media service needs of large/increasing numbers of subscribers. One instance of the OpenScape Media Server may reside upon the CMP platform; multiple instances are also possible for redundancy, scalability and optimized bandwidth utilization reasons.
- A single Common Management Platform is used to support the entire solution.

OpenScape Voice virtualized architecture

The most important features provided by virtualization are the reduced number of servers and the capability of our solution to be hardware-agnostic.

Therefore, OpenScape Voice/UC Suite operation in a virtual environment enables the following capabilities:

Server consolidation

The applications and virtual machines deployed onto a VMware host can use different guest operating systems, i.e. OpenScape Voice (Linux) and OpenScape Concierge (Windows) can both be deployed onto the same VMware host and share its physical resources.

Hardware independence

Having many hardware server vendors and models in a data center environment adds complexity and cost to the operation, therefore, customers often look to standardize their IT hardware infrastructure. Virtualization allows customers to deploy applications onto any hardware platform, assuming it has been certified by VMware and it meets the resource requirements of the application, as described in this document.

Application and server platform

At the heart of the OpenScape Unified Communications is the OpenScape Voice real-time, SIP-based, Voice over IP application that provides the carrier-grade level of redundancy, reliability and scalability required for mission-critical deployments. OpenScape Voice operates on commercial servers over QoS managed networks.

The OpenScape Voice VoIP system provides the following key features:

- SIP B2BUA
- Enterprise telephony features
- User management and address translation functions
- Interface to monitor and control media transactions including pure telephony
- Interface for advanced services, such as presence services, billing services, collaboration services, etc.
- Gateway selection and hunting
- Routing and translation functions comparable to a carrier-grade solution

OpenScape Voice is designed as an open standards platform that runs on standard rack-mountable computing hardware.

The base system software runs on the SUSE Linux Enterprise Server operating system – SLES12 64 bit. This is combined with cluster control software to run all parts of the system as a redundant unit. The system runs on a single server or a dual server cluster, depending on the number of users and customer requirements.

Hardware redundancy and cluster connectivity

OpenScape Voice controls and supervises call setup; the actual media payload (voice and/or video) is carried over the LAN/WAN between endpoints. The administration, call control, and billing traffic are carried over redundant pairs of network interface cards through redundant, interconnected L2/L3 switches that provide redundant networking.

The OpenScape Voice redundant configuration can be deployed as follows:

- Co-located cluster nodes
- Geographically separated with the cluster nodes in the same VLANs/subnets with the interconnect link served by a layer-2 connection
- Geographically separated with the cluster nodes in different VLANs/subnets with the interconnect link served by a layer-2 connection
- Geographically separated with the cluster nodes where the interconnect link is a layer-3 connection

Security

OpenScape Voice supports SRTP for media encryption. SRTP secures voice communication by encrypting the media packets between media devices.

End-to-end media encryption is implemented using a "best effort" mechanism that is dependent on SRTP support from the media devices that are involved in the connection. An encrypted SRTP connection is established when both media endpoints support SRTP and use a common key management protocol (e.g., MIKEY0 or SDES); if an SRTP connection cannot be established, the call will still be completed but with an unencrypted RTP.

SRTP MIKEY (Profile 0) is supported on connections between nearly all media endpoints of the OpenScape Unified Communications.

With OpenScape Voice, SRTP SDES (Profile 1) is supported for connections between nearly all media endpoints of the OpenScape Unified Communications solution and is the preferred SRTP key management protocol to use.

OpenScape Voice also supports media encryption for connections that are signaled over the SIP-Q interface between itself and:

- Another OpenScape Voice system
- OpenScape 4000
- OpenScape Business

Solution media devices that do not support SRTP or do not support a compatible key management protocol should negotiate down to RTP.

OpenScape Voice supports enhanced SDP backward compatibility for best effort SRTP that allows for support of third-party SIP endpoints that do not support SRTP and do not properly handle SRTP to RTP fallback which might otherwise have resulted in call failures.

SRTP requires a secure signaling connection to be used between the media device and the OpenScape Voice server. For SIP devices, TLS is used, and for the OpenScape Media Server, IPSec is used to secure the signaling connection.

All Session Border Controllers (SBCs) that are approved for use with OpenScape Voice support SRTP media encryption using transparent media relay, or "pass-through". In addition, OpenScape SBC (V2 and later) can support SRTP termination of MIKEY0 and SDES key management, which allows for SRTP to RTP termination and also SRTP mediation between MIKEY0 and SDES key exchange methods for media connections routed via the SBC. This interworking is useful, for example, to maintain maximum media stream security within the enterprise network when using SIP trunks to a service provider that does not support SRTP, or to ensure security for remote subscribers (e.g., home workers) that access OpenScape Voice via an un-secure network.

Security: TLS

OpenScape Voice provides Transport Layer Security (TLS) for protecting signaling communications on SIP endpoint, SIP server, and SIP-Q server interfaces.

OpenScape Voice also supports optional use of TLS to secure the transport of XML messages on the SOAP server management interface. This feature also provides for client user authentication and role-based authorization for controlling access to OpenScape Voice management functions.

The system's static capacity for TLS is 50,000 endpoints. Dynamic capacity depends on customer feature configuration and call rate.

Security: IPSec

OpenScape Voice supports optional use of IPSec for protecting the OpenScape Voice SOAP and SNMP management interfaces to the external OpenScape Voice Assistant and CMP, as well as for protecting the MGCP signaling interface to a media server.

Security: Event logging

Security event logging can be provided by using the standard Syslog mechanisms for both platform and application or optionally by using the Linux Audit OS module.

OpenScape Software Assurance

OpenScape Software Assurance assures that customers are kept on the latest software version of OpenScape products. Continuous software upgrades guarantee long-term software stability and up-to-date security features and improve the OpenScape Unified Communication interfaces towards other products and solutions.

Upgrade/Migration to OpenScape Voice V10

Upgrades require an upgrade license per user license purchased in the previous release.

For new installations, the current available system server deployment options are:

- Lenovo SR530
- Virtualized environment on VMware ESXi V6.7

Earlier server version simplex or duplex customers who wish to migrate to OpenScape Voice V10 software will be required to change out their platform to a supported Lenovo or Fujitsu server:

- Lenovo x3550 M5 (or M4, M3)
- Fujitsu RX200 S7 (or S6)

Network connectivity

SIP trunking to service providers

Many enterprises are already using VoIP; however, many use it only for communication on the enterprise LAN.

SIP trunking takes the VoIP concept beyond this LAN application. The full potential for IP communications can be realized only when the communication is taken outside of the corporate LAN.

The OpenScape SBC provides secure connection of OpenScape Voice to carrier-based SIP trunking services.

SIP Private Networking

SIP Private Networking uses the SIP-Q protocol currently used for OpenScape Voice-to-OpenScape Voice/4000/Business connectivity.

This protocol provides feature transparency among users in these networked systems.

QSIG networking

QSIG networking provided by the OpenScape Branch supports SIP-Q, which permits OpenScape Voice to interwork with OpenScape Voice, OpenScape 4000, OpenScape Business or a QSIG PBX.

Call Admission Control features

The integrated Call Admission Control (CAC) features provide for management of the bandwidth used for the transport of media traffic (such as RTP audio, T.38 fax, and video) through the bottleneck links that may exist in an enterprise network. This feature ensures that real-time media calls are only established when the necessary bandwidth resources are available on all access links that exist between the two communicating endpoints. The following are examples of the functionality the Call Admission Control feature provides:

- CAC rerouting to SIP subscribers or alternate SIP gateways
- Call denial
- Dynamic handling of link failures

Supported gateways

For all calls made to the Legacy PSTN TDM network, a gateway on the enterprise edge is required.

The survivable OpenScape Branch family of integrated gateways provide access to the Legacy PSTN network.

Features

Keyset telephony user features

Keyset telephone user features provide multiple line capability and other associated functions for a SIP endpoint configured as a keyset. Keysets are sometimes known as multiline telephones.

Any of the OpenScape Desk Phone CP SIP phone family can be configured as keysets.

- Audible ringing on rollover lines
- Delayed ringing
- Direct station select
- Line focus preview
- Line key operation modes
- Line reservation manual hold
- Multiline appearance
- Multiline origination and transfer
- Multiline preference keyset operation modes
- Phantom lines
- Visual indicators for line and feature key status
- Privacy

OpenScape Voice-based call forwarding user features

OpenScape Voice-based call forwarding user features provide a means to customize the handling of calls when a subscriber is unavailable to answer them. The following are the OpenScape Voice-based call forwarding user features:

- System call forwarding, internal/external – all calls (CFSIE-all)
- System call forwarding, internal/external – busy (CFSIE-busy)
- System call forwarding, internal/external – do not disturb (CFSIE-DND)
- System call forwarding, internal/external – don't answer (CFSIE-DA)
- Call forwarding – return
- Call forwarding – unreachable
- Station call forwarding – all calls
- Station call forwarding – busy line (CFBL)
- Station call forwarding – don't answer (CFDA)
- Station call forwarding – remote activation
- Station call forwarding – time-of-day
- Station call forwarding – fixed
- Station call forwarding – remote call forwarding
- Station call forwarding – voice mail

Other user features

Other OpenScape Voice user features provide additional capabilities. The following are some of the other user features provided by OpenScape Voice:

- Anonymous call rejection
- Auto Answer only for ACD calls
- Call completion on busy subscriber/no reply (CCBS/NR)
- Call pickup – directed
- Call pickup – group
- Conference, station-controlled
- Calling name delivery (CNAM)
- Calling name delivery blocking (CNAB)
- Calling number delivery (CND)
- Calling number delivery blocking (CNDB)
- Customer-originated trace
- DLS user mobility
- Do not disturb (DND)
- Executive override
- Intercom Calls
- Last Incoming Number Redial (LINR)
- Last Outgoing Number Redial (LONR)
- Multiple contacts
- Multi Level Precedence & Preemption
- Music on hold
- One Number Service
- One-Way Paging Broadcast
- Serial ringing
- Simultaneous ringing
- System speed calling
- Toll and call restrictions
- Transfer
- Transfer security
- Virtual DN

Business group features

The business group concept provides the basic capabilities for handling a group of subscribers associated with a single enterprise. It also permits OpenScape Voice to recognize the associations of the subscribers the group contains. Business group features simplify such tasks as dialing plan administration, intra-group communication, and traffic measurements. The following are the business group features:

- Attendant answering position (AAP)
- Business group access codes
- Business group account codes
- Business group authorization codes
- Business group billing
- Business group department names
- Business group main number
- Business group numbering plan
- Business group traffic measurements
- Business group web portal
- Direct inward dialing (DID)
- Direct outward dialing (DOD)
- Distinctive ringing
- Extension dialing
- Group-level feature administration
- Message detail recording
- Night bell call pickup
- Station restrictions

Other workgroup features

The following are the group features:

- Call pickup – group, directed.
- Hunt groups:
  circular,
  linear,
  UCD,
  parallel,
  manual.
- Hunt group features:
  make busy,
  music on hold,
  night service,
  no answer advance,
  overflow,
  queuing,
  stop hunt,
  traffic measurements
- Call Park:
  Park to System

Routing and translation features

Routing and translation features provide such capabilities as public numbering plan compliance and routing that varies depending upon such factors as origin, traffic, and time of day. The following are the routing and translation features:

- A-side signaling-based routing
- Alternate routing
- Alternate routing with overflow among route types
- Call diversion for invalid destinations
- Cost-effective routing
- Digit modification for digit outpulsing
- E.164 compliance
- Intercept treatment
- International translation support
- Leading digit and most-matched digit translation
- Media server digit map management
- North American Numbering Plan compliance
- Numbering plans, business group
- Origin-dependent routing
- Rerouting based on SIP response codes and WAN outages
- Source-based IP routing
- Subscriber routing options ENUM (electronic number mapping)
- Time-of-day routing
- Vertical service codes
- Voice VPN

CDR features

CDR features simplify call tracking and billing for OpenScape Voice.

The following are the CDR features:

- Call detail record generation
- Intermediate long duration records
- Message detail recording
- Usage reporting
- QoS Data in CDR Records

Security features

Security features provide security for various aspects of the system, such as billing records, data files, and administration interfaces. The following are the security features:

- Account and password management security
- Billing records security
- Data file security
- Defending denial of service attacks
- Event logging
- File transfer security
- FIPS 140-2 compliant
- Hypertext transfer protocol over SSL
- IPSec baseline
- Login categories
- Media stream security
- OpenScape Voice Assistant security
- Provisioning and security logging
- Secure CLI
- Secure Shell on the OpenScape Voice Assistant interface
- Secure storage of CDR password
- SIP privacy mechanism
- TLS support – network connections
- TLS support – subscriber access
- VLAN provisioning

Serviceability features

These features provide mechanisms to improve serviceability, such as diagnostics and debug tools, code controls, and administrator controls. The following are the serviceability features:

- Administrator identification and authentication
- Backup and restore
- Basic traffic tool
- Call trace
- Continuous trace
- Database versioning
- Log file retrieval tool
- Maintenance manager
- Mass provisioning
- On-demand audits
- Process debug tool
- Query of subscriber transient operational status
- RapidStat
- Real-time trace
- Remote patching
- Remote restart
- Software installation
- System software and patch level status
- System upgrade

SIP signaling features

These features support SIP signaling and the interworking with other elements such as application servers, voice conferencing applications, and voice mail systems. The following are the SIP signaling features:

- Integration with OpenScape Xpressions
- Interworking with OpenScape SBC
- Interworking with SIP service providers
- Interworking with unified messaging systems
- Interworking with voice mail systems
- AS-SIP support
- SIP over TCP/TLS support
- SIP privacy mechanism
- SIP REFER method support
- SIP session timing
- SIP UA registration renewal during WAN outage
- SIP-Q interworking for feature-rich connections to other Unify communication systems
- SIPREC interworking with Voice Recording (limited)

CSTA support features

OpenScape Voice provides a standard European Computer Manufacturers' Association (ECMA) Computer Supported Telecommunications Applications (CSTA) protocol interface to external CTI applications. The following are examples of the functionality that the CSTA support features provide:

- CSTA services support
- Application-provided caller identification
- Flexible digit processing
- Integration with Fault Management
- Message waiting indicator
- One Number Service
- OpenScape Voice-provided calling name
- Private network number support

System functions and features

These features support such tasks as alarm reporting, message waiting indicator control, and recovery handling. The following are the system functions and features:

- Agent for OAM&P
- Alarm reporting
- Announcements
- Data synchronization
- Display number modification
- Emergency calling
- Feature execution for unreachable subscribers
- Internal audits
- Interworking with automated attendant systems
- Local management
- T.38 fax support
- Media server support
- Message waiting indicator
- Multiple language announcements
- Multiple time zone support
- Overload handling
- Recovery handling
- SDP transparency
- Silence suppression disabling
- SOAP interface
- System history log

System capacities

Parameter[1]	OpenScape Voice Standard Duplex	OpenScape Voice Integrated Simplex
TCP Connections	327,681	5,000
TLS sockets	50,000	5,000
Unique keyset DNs	100,000	5,000
Average keyset line appearances	2	2
Business Groups	6,000	600
Numbering Plans	5,999	600
Total trunks (SIP and SIP-Q) Standard PBX[2]	60,000	5,000
Total trunks (SIP and SIP-Q) Tandem[2]	60,000	5,000
Total SIP-Q trunks[2]	20,000	5,000
Prefix Access Codes	35,000	18,000
Destination Code table entries	200,000	10,000
Destinations (two routes per destination average)	54,000	27,000
Route Lists	54,000	27,000
Routing Areas	30,000	15,000
Classes of Service	30,000	15,000
Number of Hunt Groups	25,000	1,250
Hunt Group size	2,048	200
Hunt Group memberships per subscriber	32	32
Number of Pickup Groups	10,000	1,000
Pickup Group size	64	64
Pickup Group memberships per subscriber	1	1
Maximum Station Controlled Conference participants	16	16
Feature Profile per subscriber	1	1
Simultaneous SIP-Q calls half calls (max.)	20,000	5,000
Simultaneous SIP-Q calls tandem (max.)	10,000	5,000
Simultaneous SIP-Q calls (SIP + SIP-Q)	60,000	5,000

1 Some of the numbers are extrapolated from standard installation

2 Recommended limits, not enforced

Supported RFCs

Supported SIP-related RFCs

- RFC 2976 – SIP INFO method (e.g. for SIP-Q
- RFC 3261 – SIP
- RFC 3262 – Limited support of PRACK for RFC 3262, 100rel
- RFC 3263 – Server location
- RFC 3264 – Offer-answer model for SDP
- RFC 3265 – SUBSCRIBE/NOTIFY method, Events
- RFC 3311 – UPDATE method
- RFC 3323 – Privacy header field
- RFC 3325 – P-asserted identity header field
- RFC 3326 – Reason header field
- RFC 3515 – SIP REFER method
- RFC 3891 – Replaces header field
- RFC 3892 – Referred-by header field
- RFC 3903 – PUBLISH method
- RFC 3911 – Join header field
- RFC 4028 – SIP session timers
- RFC 4092 – ANAT in SIP
- RFC 5630 – SIP-SIPS
- RFC 5806 – Diversion header field
- RFC 5876 – Updates to Asserted Identity
- RFC 5923 – Connection reuse
- RFC 5954 – Essential correction for IPv6 ABNF and URI compari-son rules
- RFC 6086 – SIP INFO packages

Supported SDP-related RFCs

- RFC 2327 – SDP
- RFC 3266 – Support for IPv6
- RFC 3605 – RTCP attribute in SDP
- RFC 3890 – Transport-independent bandwidth modifier
- RFC 4091 – Alternative Network Address Types (ANAT)
- RFC 4566 – SDP-new
- RFC 4567 – Key management extensions
- RFC 4568 – Security descriptions (SDescriptions)

Supported event-package RFCs

- RFC 3842 – Message waiting indication
- RFC 4235 – INVITE-initiated dialog event package
- RFC 4575 – Conference event pack-age
- RFC 6035 – RTCP summary event package