A MITEL
PRODUCT
GUIDE

Unify OpenScape Session Border Controller

OpenScape SBC V11

Installation Guide

04/2025

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contents

1 OpenScape Session Border Controller– Introduction

OpenScape Session Boarder Controller (SBC) is a security device which enables Voice over IP networks to extend Session Initiation Protocol (SIP) based applications beyond the Enterprise network boundaries, for example, when SIP clients of a Openscape Voice system reside in different IP networks.

1.1 About This Guide

This book guides installation personnel through the process of installing the hardware and software up to and including the point where provisioning can begin and the expanded network components can be installed and verified. The user must refer to the provisioning and expanded network component document (s) to support that phase of the system installation process.

Intended Audience

Prerequisite Knowledge

The audience for this guide is Unify Professional Services and Back Level Support personnel. Note that this does not preclude other Unify personnel, customers, or third-party service providers who have the necessary prerequisite knowledge from using the guide.

This guide is written to the user who has:

- Successfully completed the Unify OpenScape Voiceand OpenScape SBC installation and technical training courses.
- Advanced SuSE Linux (OpenSuSE) operating system and Microsoft Windows operating systems knowledge and experience.
- Basic knowledge of the third-party platforms and equipment used for OpenScape Voiceand OpenScape SBC including: their physical characteristics, their assembly, their documentation (installation, service, and troubleshooting), and the documentation web sites associated with the third-party platform and equipment manufacturers.
- Basic knowledge of the industry standards and specifications utilized by OpenScape Voiceand OpenScape SBC and associated equipment.

The procedures in this guide require an understanding of and adherence to local safety practices, the safety practices identified in this guide, and the safety practices identified in the third-party documentation.

1.2 Security Information

Refer to the OpenScape Session Boarder Controller Security Checklist - Planning Guide for the measures to be taken to secure OpenScape Session Boarder Controllers (SBC).

IMPORTANT: It is of vital importance that security measures outlined in the Security Checklist are executed.

In addition, other security measures should be taken to secure the network used for the OpenScape Voice solution.

1.3 Safety Information and Warnings

The procedures in this documentation require an understanding of and adherence to local safety practices, the safety practices identified in this documentation, and the safety practices identified in the third-party documentation.

Special Notices

Safety

General Safety

Potentially dangerous situations and information of special importance are noted throughout this documentation. The following alert indicators are used:

IMPORTANT: An important notice calls attention to conditions that, if not avoided, may damage or destroy hardware or software, or may result in unrecoverable data loss

NOTICE: A "note" notice calls attention to important additional information

The following information is included in this publication for the use and safety of installation and maintenance personnel:

- Do not attempt to lift objects that you think are too heavy for you.
- Do not wear loose clothing; tie back your hair while working on machines.
- Wear eye protection when you are working in any conditions that might be hazardous to your eyes.
- After maintenance, reinstall all safety devices such as shields, guards, labels, and ground wires. Replace worn safety devices.
- If you feel any action is unsafe, notify your manager before proceeding.
- Do not use a telephone to report a gas leak while in the vicinity of the leak.

Safety with Electricity

General Installation

High Voltage

CAUTION

- Risk of Explosion if Battery is replaced by an incorrect type

  Dispose of used batteries according to the instructions
- Only qualified service personnel should install this device. Users should not attempt to perform this function themselves. The installer must ensure that the equipment is permanently connected equipment, pluggable type B or connected to a socket-outlet that has been checked to ensure that it is reliably earthed in accordance with national electric codes.

- The power outlet socket must be located near the equipment and must be easily accessible.
- Size a length of green-with- yellow stripe copper ground wire to run from protective earth marked terminal to the existing or planned grounding system. The ground wire must be a minimum of 18 AWG recommended for runs up to 45m (~150ft)
- Caution: to reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified telecommunication line cord
- Observe all safety regulations and read the warnings, cautions, and notes posted on the equipment.
- Find the switch to power off the cabinet. Read the posted instructions.
- Ensure that a machine cannot be powered on from another source or controlled from a different circuit breaker or disconnecting switch.
- When a procedure requires that you power off the system:
  - Lock the wall box-switch in the off position.
  - Attach a DO NOT OPERATE tag to the wall box-switch.
- Do not work alone. Work with another person who knows the locations of the power-off switches, especially if you are working with exposed electrical circuits.
- Follow the instructions in the manual carefully, especially when working with circuits that are powered. Disconnect power when instructed to do so in the procedures
- Disconnect all power before working near power supplies unless otherwise instructed by a maintenance procedure.
- Disconnect all power before installing changes in machine circuits unless otherwise instructed by a maintenance procedure.
- High voltages capable of causing shock are used in this equipment. Be extremely careful when measuring high voltages and when servicing cards, panels, and boards while the system is powered on.
- Do not wear jewelry or other metal objects.
- When possible, work with one hand so that a circuit is not created. Keep the other hand in your pocket or behind your back.
- Use caution when installing or modifying telephone lines. Never install telephone wiring during an electrical storm.
- Never install a telephone jack where it can get wet unless the jack is specifically designed for wet conditions.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Avoid using a telephone (other than the cordless type) during an electrical storm due to the remote risk of shock from lightning.

Equipment Room

- Look for hazards in your area and eliminate them. Examples are moist floors, ungrounded power extension cables, power surges, and missing safety grounds.
- Rubber electrostatic mats will not protect you from electrical shock. Do not use them for this purpose. Stand on suitable rubber mats to insulate you from grounds such as metal floor strips and machine frames.
- Do not use tools covered with a soft material that does not insulate you when working with powered circuits. Use only tools and testers suitable for the job, approved by Unify.
- Do not use worn or broken tools or testers; inspect them regularly.

- Set controls on testers correctly and use approved probe leads and accessories intended for that tester.
- The surface of a mirror is conductive. Do not touch powered circuits with a mirror. To do so can cause personal injury and machine damage.
- Do not store combustible gases or flammable materials in cabinets near the site.

Emergencies

What to Do in and Emergency

- In the event of an accident, use caution and remain calm and controlled.
- Always switch of the power supply before touching the victim.
- If you are not able to disconnect the power supply, use a nonconductive object, such as a wooden rod, to push or pull the victim away from electrical contact.
- Administer **First Aid**.
- Immediately **Call for Help**.

First Aid

- Be familiar with basic first aid procedures for electrical shock. A fundamental knowledge of various resuscitation methods if the victim has stopped breathing or if the victim’s heart is no longer beating, as well as first aid for treating burns, is absolutely necessary in such emergencies.
- If the victim is not breathing, immediately perform mouth-to-mouth or mouth-to-nose resuscitation.
- If you are trained and certified, administer cardiac compression if the victim’s heart is not beating.

Call for Help

- Immediately call a rescue group, ambulance or hospital. Provide the following information in the following sequence:

  - Where did the accident happen?

  - What happened?

  - How many people were injured?

  - What type of injuries?

  Wait for questions

Reporting Accidents

- Report to your manager all accidents, near accidents, and possible hazards to ensure their causes are resolved as soon as possible.
- Report any electric shock, no matter how small.

1.4 OpenScape Session Border Controller — Overview

The OpenScape Session Border Controller (SBC) deployment in the OpenScape Voice environment is supported in a centralized location (same location as the OpenScape Unified Communication (UC) server, i.e. the customer’s Data Center). There are several deployment scenarios and OpenScape SBC runs on different hardware platforms depending on the number of SBC sessions required. OpenScape SBC is a component of the

OpenScape Solution Set, and is backward compatible with prior OpenScape Solution Set versions.

Functional Overview

OpenScape SBC is a software-based network border element designed to deliver superior Voice over IP (VoIP) security and cost savings for the OpenScape Enterprise Solution set. It enables OpenScape SIP-based communication and applications to be securely extended beyond the boundaries of an enterprise network.

For deployment scenarios that require a centralized SBC, OpenScape SBC performs the necessary interoperability, security, management, and control capabilities to support SIP trunking applications. It also supports the SIP endpoint registration services that are necessary to support remote user and branch office applications. OpenScape SBC performs SIP deep-packet inspection specifically tailored for the OpenScape Voice environment that is necessary to provide proper mediation between IP networks, such as the mapping of IP addresses and ports within SIP signaling and RTP/SRTP media packets that allows for NAT traversal. Media anchoring can be configured to the extent required by media control policies (for example, for NAT traversal), or set to allow direct media connections between clients.

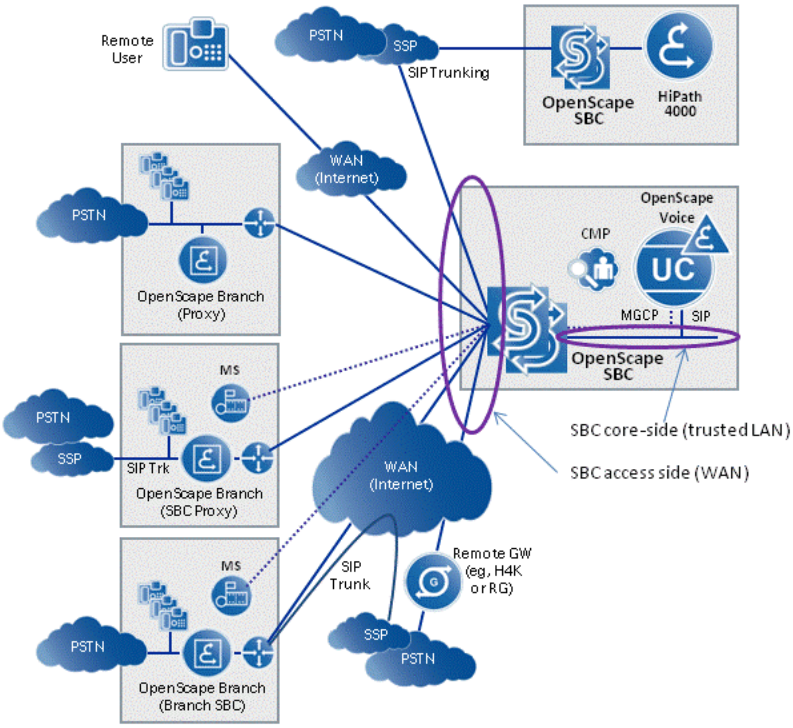
OpenScape SBC enhances customer-network security by providing SIP-aware security functionality including dynamic opening and closing of “pinholes” for media connections, stateful SIP protocol validation, Denial of Service (DoS) mitigation, and network topology hiding. It also supports TLS encryption on both the core- and access-side SIP signaling interfaces as well as SRTP media encryption for both transparent relay pass-through and termination/mediation scenarios.

OpenScape SBC facilitates SIP trunk interfaces to SIP Service Providers (SSPs), connection to remote user SIP phones, for example for home workers accessing an OpenScape Voice system over an Internet connection, and for connection to OpenScape Branch systems serving remote branch locations.

OpenScape SBC is specifically designed for use as a centralized SBC in the OpenScape solution environment. In other words, the OpenScape SBC is designed to be deployed in the same location as the OpenScape UC server, for example, in the customer’s data center.

OpenScape Branch can provide SBC functionality in “non-centralized”, ie, branch office, locations.

The diagram below illustrates the deployment scenarios supported by OpenScape SBC:



- The **Session Border Controller** (SBC) provides security functions such as Firewall and Virtual Private Network (VPN) while interfacing with a public network.
- The OpenScape SBC is fully manageable via a local web based Graphical User Interface (GUI) or via the **Common Management Platform** (CMP) as a single network element on the inside LAN network, making it easy to manage together with the other OpenScape solution components that comprise the Enterprise Network. OpenScape SBC also supports a local management via a web based Graphical User Interface (GUI) using HTTPS.
- The OpenScape SBC currently shares common support tools with OpenScape Branch.
- **OpenScape SBC** can be deployed within a trusted network, to untrusted networks or a mixed deployment can be used. In a trusted network all VoIP users are within the trusted Enterprise network. When interfacing to untrusted networks an Internal OpenScape SBC Firewall/NAT is used when providing VoIP service to users outside the trusted Enterprise WAN. A separate Firewall is required to support non-VoIP access, e.g., management and billing.
- A single **OpenScape SBC** can communicate to one OpenScape UC server. Multiple OpenScape SBCs can be configured to provide increased capacity as long as the SBC traffic is split e.g., a separate SBC for two different SIP Trunk Service Providers.
- The OpenScape SBC is offered on three **HW platforms** allowing a maximum SBC session capacity of up to 1200 and 4000 SBC sessions.

NOTICE: Please note that number of concurrent SBC sessions required is based on many factors but not limited to the number of remote users, SIP trunking and OpenScape Branches.

- An **SBC Session** is defined as an active SIP call connection that is being managed and processed by the OpenScape Session Border Controller. Each SIP call connection may be consisting of the SIP signaling packets only (when media packets are being routed between the endpoints), or when both SIP signaling and media packets being handled through the OpenScape Session Border Controller.
- **OpenScape SBC** supports several redundancy scenarios based on the deployment of OpenScape Voice and data centers in the customers network. SBC redundancy can be applied to simplex OpenScape Voice systems and Co-located Duplex OpenScape Voice systems.

Software Licensing

OpenScape Session Branch deployment requires licensing of the product. A CAPEX licensing model and OPEX mode is used for Enterprise and hosted environments.

1) **CAPEX Licensing**

   CAPEX licensing is used for Enterprise environments where the customer owns the licenses and does not wish to lease the licenses on a monthly basis. The following license type are associated with OpenScape SBCs:

   - **OpenScape SBC Base**
   - **OpenScape SBC Session License** (used for OpenScape Branch and OpenScape SBC)
   - **Circuit Telephony Connector** (used for SIP sessions of OpenScape Branch and OpenScape SBC or used for Circuit Telephony Sessions of UTC and ATC)

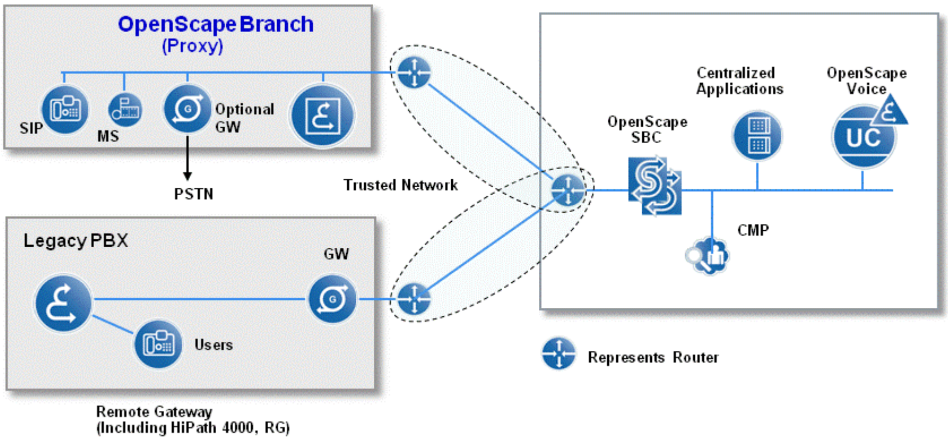
2) **OPEX Licensing**

   OPEX licensing is used for Enterprise environments where the customer wishes to lease the licenses on a monthly basis and consists of two parts:

   - **Product Instance** - The Product Instance is purchased once for each product and consists of all of the licenses necessary to equip a product for its maximum capacity, including all major features. The Product Instance enables the Monthly Subscription Licenses for the OpenScape SBC.
   - **Subscription License**-The Subscription License is the monthly charge for a single user to use a single product. If a single user has voice, voice mail and Unified Communications (UC), then they would pay for 3 Subscription Licenses – one for OpenScape Voice, one for OpenScape SBC and one for OpenScape UC. The Subscription Licenses are based upon the product usage that is reported monthly and the billing is calculated on actual service consumption.

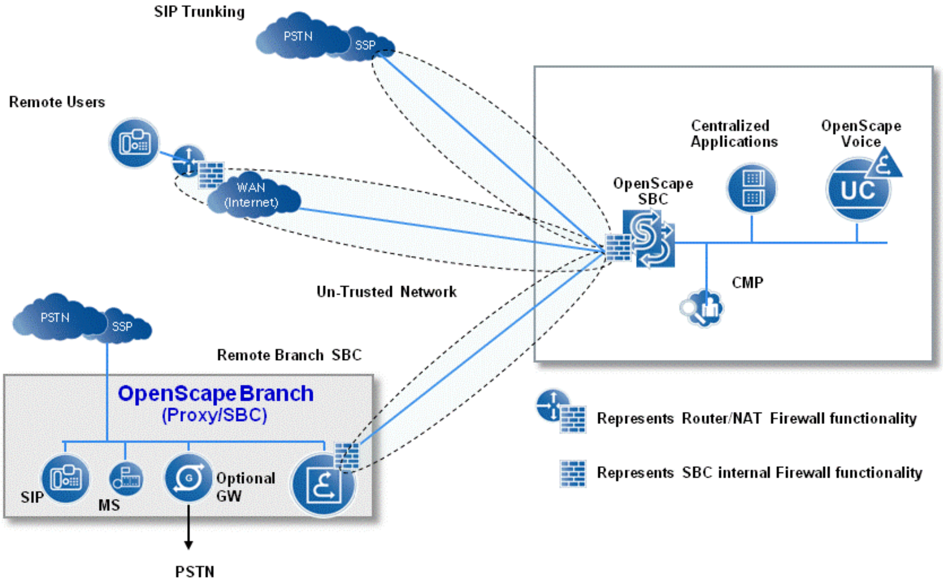
OpenScape SBC in the Network

The figure below shows deployment in a trusted network with the SBC connected directly to the WAN. This deployment is possible for scenarios where all VoIP users are within a trusted Enterprise Network.



The figure below shows deployment in an untrusted network with the SBC behind an IT Firewall/NAT. This deployment is typically required by customers when providing VoIP service to users outside the trusted Enterprise WAN.

SIP and MGCP ALG or helpers must be disabled within the external firewall as this configuration is not supported.



A mixed deployment can be used, with VoIP via the Internet or other service providers' networks connecting via the internal Firewall, and user within the Enterprise WAN connecting directly to the WAN side of the SBC.

OpenScape SBC Signaling Transport - Overview

OpenScape SBC supports signaling transport using TCP and transport signaling security using Mutual Authentication TLS (MTLS) and Server Authentication TLS (TLS). The following signaling transport and signaling transport security configurations are supported in the network between OpenScape and SBC networks.

Access/Peer	Core	Comments
TCP	TCP	Supported
TCP	MTLS	Supported
TLS	MTLS	Supported
TLS	TCP	Not Supported (V1)
TLS	TCP	Supported (V2)
MTLS	TLS	Supported (V2)
MTLS	MTLS	Supported (V2)

Signaling and Media Transport Protocol

OpenScape SBC - supports the following SIP signaling and media transport protocols.

Deployment Scenario	Pass-through or Termination	SIP Signaling Transport		Media Transport	
		Core	Access	Core	Access
SIP Trunking	Pass-through	TCP or UDP	TCP or UDP	RTP	RTP
		TLS *	TLS *	SRTP *	SRTP *
	Termination	TLS *	TCP * or UDP *	SRTP *	RTP *
		TCP	TLS	RTP	SRTP (Mikey0 or SDES)
Remote User and OpenScape Branch	Pass-through	TCP, TLS or UDP *	TCP, TLS or UDP *	RTP	RTP
		TLS	TLS	SRTP Mikey0	SRTP Mikey0
		TLS	TLS	SRTP SDES	SRTP SDES
		TLS	TLS	SRTP SDES	SRTP Mikey0
		TLS	TLS	SRTP Mikey0	SRTP SDES
	Termination	TCP *	TLS *	RTP *	SRTP (Mikey0 or SDES) *
		TLS *	TCP *, TLS* or UDP *	SRTP (Mikey0 or SDES) *	RTP *
Remote Standalone SIP-Q Gateway	Pass-through	TCP*	TCP*	RTP*	RTP*
	Termination	TCP*	TLS*	RTP*	SRTP* (Mikey0)

Beginning with V8 the OpenScape SBC allows separation of signaling and media flows on the access realm for remote endpoints. For example, Signaling may be utilize a MPLS or VPN connection while the RTP media is supported:

- In the same network as the signaling connection.
- An IP address which is different than the SIP signaling address in the same network, but on a different subnet.
- Signaling is supported by private IP addresses (MPLS or VPN) while the media is supported in the public address space.

IMPORTANT: Use of TLS or TCP is highly recommended over UDP.

NOTICE: Best effort scenarios could be downgraded to RTP on either side.

NOTICE: Audio and video codecs are negotiated end to end.

NOTICE: * Indicates not supported in OpenScape SBC V1

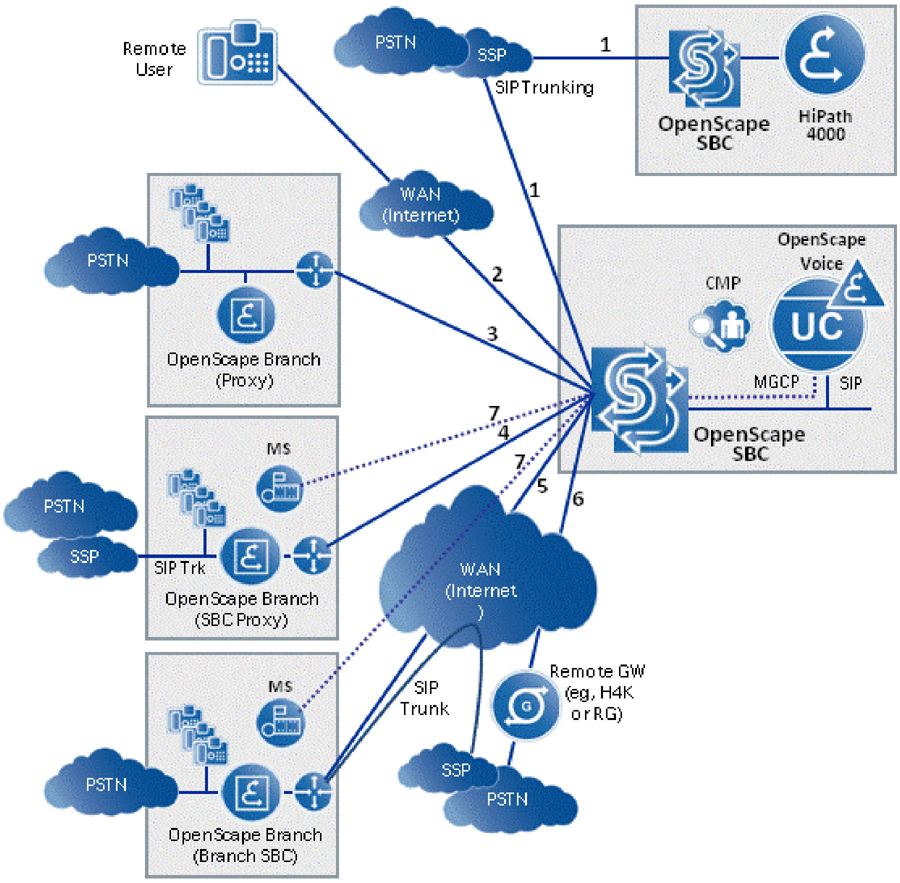
Media “pass-through” refers to OpenScape SBC V1 handling of the media packet payload whereby the unencrypted RTP or encrypted SRTP data that are received from the connected endpoints are relayed through the SBC without modification. OpenScape SBC does not play a role in reformatting of the actual media payload so the media format, including negotiation of codec and encryption is performed between the media endpoints. This implementation allows for SRTP media encryption to be realized across the entire end-to-end path of the media connection, assuming that the connected endpoints support SRTP using a compatible key management protocol.

Media Transcoding

Effective with OpenScape SBC V8 support of media transcoding is realized. Transcoding is supported between the OSV solution supported codecs G.711 (a-law, u-law), G.729 and G.722 and the iSAC and iLBC codecs of the WebRTC open-source project which shall be implemented in OSMO. The media transcoding mechanism makes use of the concept of administered Media Profiles.

Deployment Scenarios — Overview

OpenScape Session Border Controller deployment in the OpenScape Voice environment is supported in a centralized location only, that is in the same location as the OpenScape UC server (e.g., in the customer’s Data Center) for the following deployment scenarios.



1) **SIP Trunking to a SIP Service Provider (SSP)**

- Provides secure connection of OpenScape Voice and OpenScape 4000 IP telephony solution to carrier-based SIP trunking services that provide access to the Public Switched Telephone Network (PSTN).
- OpenScape SBC also provides for compatibility with the SIP signaling variations support by various SSPs.
- Used also for private SIP trunking connections between Enterprise VoIP Networks.

2) **Remote User (e.g. home worker)**

- Provides secure remote user access to the IP telephony infrastructure of an OpenScape Voice system for SIP phones regardless of location.
- Supports the necessary near-end and far-end Network Address Translation (NAT) traversal functions for connection using public IP addresses via the Internet. OpenScape SBC can be installed behind an external near-end NAT/firewall, for example, inside the customer’s DMZ. OpenScape SBC can also support remote users that are installed behind a far-end NAT/firewall.
- Symmetric Response Routing is used by OpenScape SBC to dynamically detect the SIP signaling IP address/port of a remote user behind a far-end NAT which is used to send SIP responses. Symmetric RTP is used similarly for the media payload.
- All OpenScape Voice SIP subscriber features are supported by OpenScape SBC for a Remote User.

3) **Remote OpenScape Branch (Proxy)**

   - Facilitates the connection of remote branch offices that use OpenScape Branch operating in proxy mode connected with the headquarters via the private enterprise network, and is therefore using the same IP address space.
   - OpenScape SBC is usually optional in this configuration since there is typically no NATing to be performed; however, an OpenScape SBC may be used, for example, when the remote OpenScape Branch system that is operating in proxy mode because it is installed behind a DSL router (with a static or dynamic IP address) at the branch office. Use of OpenScape SBC may also be desired for serviceability and/or security reasons in cases when there is no NATing to be performed.

4) **Remote OpenScape Branch (SBC Proxy)**

   - Facilitates the connection of remote branch offices that use OpenScape Branch operating in proxy mode connected to the central headquarters via the enterprise network, and is therefore using the same IP address space.
   - OpenScape SBC is optional in this configuration since there is no NATing to be performed; however, use of OpenScape SBC may be desired for serviceability and/or security reasons.
   - The Remote OpenScape Branch provides secure SBC connection to carrier-based SIP trunking services that provide access to the Public Switched Telephone Network (PSTN).
   - The Remote OpenScape Branch also provides SBC functionality for compatibility with the SIP signaling variations support by various SSPs.

5) **Remote OpenScape Branch (Branch SBC)**

   - Facilitates the connection of remote branch offices that use OpenScape Branch operating in SBC mode connected to the central headquarters via a WAN, such as an untrusted or public network.
   - The OpenScape SBC is required for NATing and security at the data center, as is the integrated SBC in the OpenScape Branch required for NATing and security at the remote branch office. The NAT device serving a branch location must may be configured with either a static or dynamic IP address.
   - The Remote OpenScape Branch can provide a secure SBC connection to carrier-based SIP trunking services that provide access to the Public Switched Telephone Network (PSTN).
   - Overlapping IP Address Ranges are supported at the different branch offices.

6) **Remote Gateways (not behind OpenScape Branch)**

   - Facilitates the connection of remote SIP-Q gateways, such as HiPath 3000, OpenScape 4000, or RG gateways, which are connected to the central headquarters via a WAN, such as an untrusted or public network.
   - The OpenScape SBC is required for NATing and security at the data center.

7) **MGCP Signaling support for remote Media Servers**

   - Facilitates the connection of a remote branch office that requires services from an external OpenScape Media Server connected to the central headquarters via the enterprise network or WAN. In this case the OpenScape SBC supports the MGCP signaling connection between the OpenScape Media Server located at the branch office and the OpenScape Voice system located at the central headquarters.

- OpenScape SBC is optional when the connection is via a trusted enterprise network and there is no NATing to be performed; however, the SBC may still be desired for serviceability and/or security reasons.

Any combination of the above supported deployment scenarios can be supported using the same OpenScape SBC provided that the IP address(es) of the WAN interface are on a common network for the deployment scenarios that are being used.

In cases where the deployment scenarios interface different networks having different IP address space on the SBC’s WAN interface (for example, an SSP that delivers SIP trunk services via MPLS and requires the SBC’s WAN interface to be assigned a private IP address on the SSP’s network together with Remote Users that require a public Internet IP address to access the SBC’s WAN interface), there are several options:

- Multiple OpenScape SBCs; one for each different WAN network.
- A single OpenScape SBC can be configured to logically separate the one physical OpenScape SBC access interface (eth1) into one or more VLAN 802.1q tagged private networks plus a default public network (not 802.1q VLAN tagged). IP packets on the OpenScape SBC access interface are exchanged via the local external L2 managed switch, which is configured to forward IP messages to specific L2 ports based on the VLAN tag. In the process of forwarding the IP message the VLAN tag may be removed. OpenScape SBC requires that each supported VLAN have a unique (VLAN independent) WAN IP address configured on OpenScape SBC. Each server on the respective VLAN would be required to use this WAN IP address to communicate with the OpenScape SBC).
- Starting in V8 an additional option is in place of VLAN tagging (or used in conjunction if needed), the physical network separation is performed with the OS-SBC supporting more than one physical Ethernet interface for the OS-SBC access. Starting at physical interface eth2, each physical interface added to the configuration is capable of supporting a mixture of 802.1q VLAN and non-VLAN tagged networks.

Untrusted WAN networks for which an SBC is required are:

- Internet
- SIP Service Provider Network
- Extensions of corporate IP networks to remote locations or remote users which the customer’s IT organization does not consider sufficiently secure, thus further security measures are necessary for VoIP deployment.

Trusted WAN networks for which an SBC is optional are:

- Virtual Private Networks (VPNs). If OpenScape SBC is used in a trusted WAN network that uses VPNs, since OpenScape SBC can support only a signal VPN connection, a VPN concentrator must be used on the access side of the OpenScape SBC.
- Extensions of corporate IP networks to remote locations or remote users which the customer’s IT organization does consider sufficiently secure, thus either no further security measures are necessary or there are limited select security considerations.

Multiple OpenScape SBCs can be deployed on a single OpenScape Voice system; however, routing of traffic to the desired SBC is static based upon the system and user configuration. Multiple OpenScape SBCs can be used in projects that have SBC capacity requirement that exceed the capacity limits of a single OpenScape SBC.

A single OpenScape SBC cannot serve multiple OpenScape Voice systems.

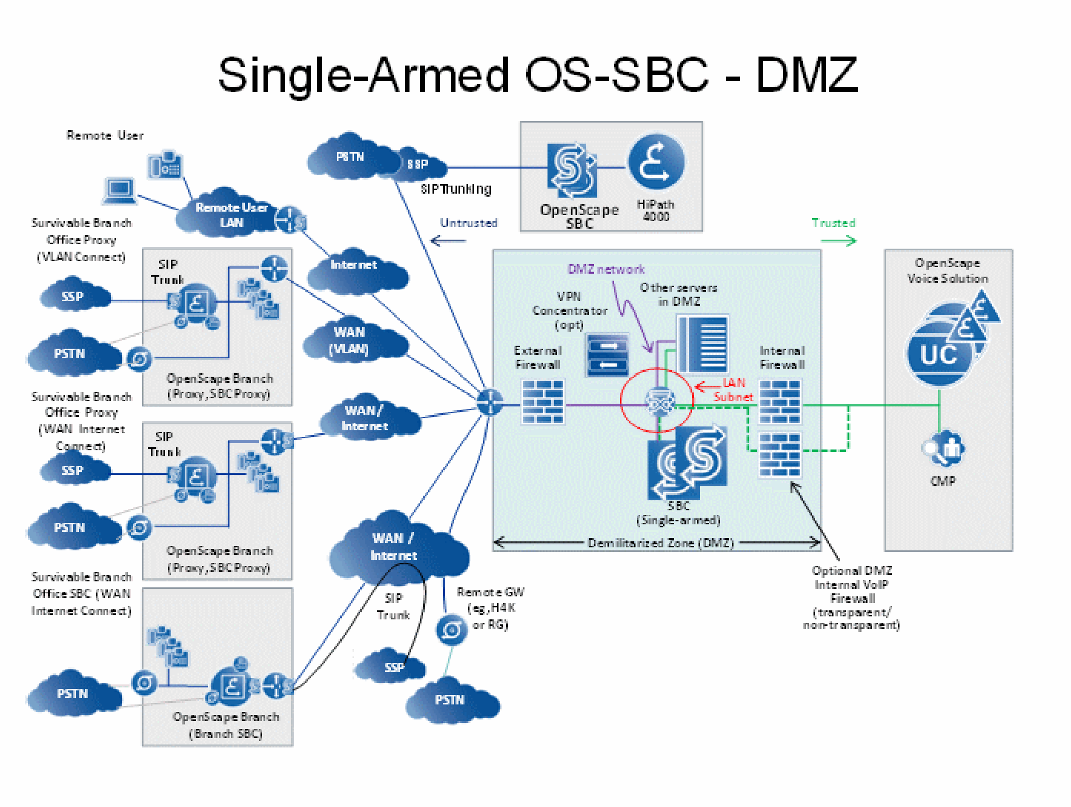
An OpenScape SBC can be deployed in a single-server configuration, or as a redundant server pair (cluster) using a VRRP-like connection for active-standby operation to achieve high availability. For OpenScape SBC redundant servers must be installed on the same subnet.

OpenScape SBC V2 supports co-located and geographically-separated duplex OpenScape Voice systems with SBCs running in either active-standby mode or active-active mode.

The OpenScape SBCis designed as a border element that sits between two different IP networks and therefore requires separate interfaces be used for the access-side (WAN) and core-side (LAN) connections. Connecting OpenScape SBC using a single interface, which would require both the access-side (WAN) and core-side (LAN) to be on the same IP network, is not supported prior to V8.

While the preferred installation approach is to use OpenScape SBC as the VoIP firewall on the WAN (access side) boundary of the data center in parallel with the customer’s data firewall, OpenScape SBC can be installed (behind) the data firewall (i.e., in the customer’s DMZ).

Starting in V8 a configuration called "Single-Armed SBC within DMZ" is supported.In this arrangement both the SBC core and access network realms are supported by a single network interface within the same IP subnet. A secondary feature allows both Ethernet eth0 and eth1 network interfaces, or all available Ethernet network interfaces be bonded or teamed together to support the IP traffic loads for a single-armed OS-SBC configuration, as well as prevent an SBC node Loss of Service in the event of a single Ethernet NIC failure or local loss of connectivity.



A simplified example is shown where the OpenScape SBC supports a single network for both the core realm and access network realm interface. A single IP address is used for both realms however this may not always be possible due to the many possible network combinations and SBC feature support. For example the existing OpenScape SBC features may become overly complex in support of such a single IP approach:

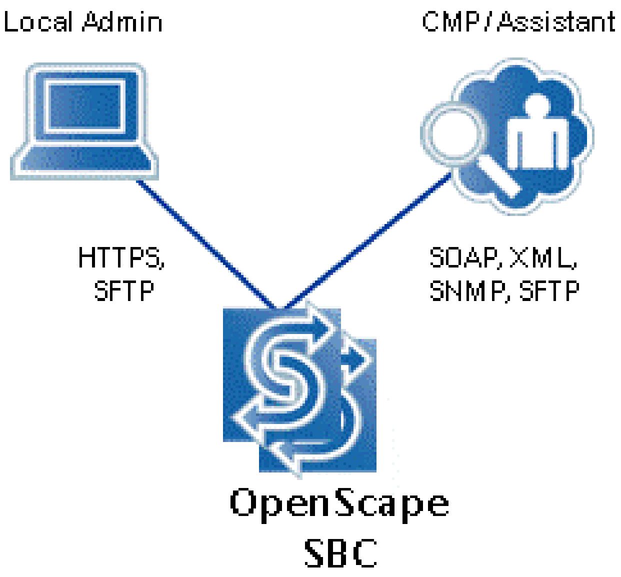
- Near-End NAT: Identifying the firewall SRC-NAT requirements may introduce a complex firewall configuration and likely require a complex SIP-ALG requirement which cannot be supported. A better approach would be to allow the OS-SBC perform Near-End NAT, i.e. Near-End NAT support may also be required for the inside facing firewall in some customer DMZ networks. Where near-end NAT is not used the firewall shall operate in a “transparent mode”.
- 802.1Q VLANs: The OS-SBC currently supports VLAN tag association by using a unique OS-SBC IP address. Using a single IP for the VLANS cannot be supported without introducing additional VLAN feature support.

Management

OpenScape SBC can be managed centrally by the Common Management Platform (CMP) with OpenScape SBC Assistant using SOAP and XML. It also supports a local management via a web based Graphical User Interface (GUI) using HTTPS.

Alarms are supported via SNMP traps to the CMP / Assistant.

OpenScape SBC supports secure file handling when transferring files using the Secure File Transfer Protocol (SFTP).



NOTICE: DLS uses the customer’s data network to manage OpenStage phones. For remote OpenStage phones that access OpenScape Voice via OpenScape SBC, the DLS traffic is not routed through the OpenScape SBC, but rather through the customer’s data firewall. If the remote users are behind a NAT/ Firewall then the DLS/phones have to use a 'Contact Me Proxy' to allow DLS to manage the phones.

Redundancy

There are various options for deploying redundancy based on the customers network, location of data centers and number of data centers. The basic configurations for redundancy are:

- SBC Server Redundancy on the same Subnet (SBC Luster)
- SBC Redundancy support for L3 geographically-separated OpenScape Voice nodes.

OpenScape Session Border Controller Redundancy Support

Redundant OpenScape SBC configurations provide VIP address failover for both LAN network and WAN addresses.

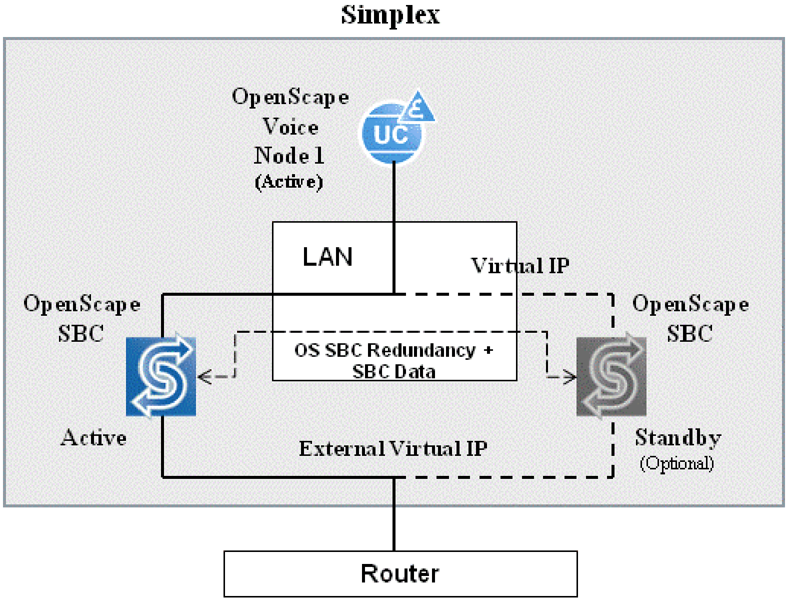
Periodic heartbeats are sent by the Standby OpenScape SBC node to detect failover conditions. Either OpenScape SBC node may assume active or standby mode at any time, however only one node shall be in an active operation mode.

When the redundant OpenScape SBC nodes share the same sub-net for the inside network additional data is synchronized in near real-time between the OpenScape SBC nodes to allow continued operation when the standby OpenScape SBC node must assume an active OpenScape SBC node status. The synchronization data includes for example:

- Configuration changes

- SIP dialog context information to allow existing SIP dialogs (creation, establishment and termination) continue after an SBC failover
- Media port mappings for sessions traversing the SBC.
- IP addresses and ports used for established TCP connections
- TLS session handles using TCP connections
- Updates to any current SIP registration bindings

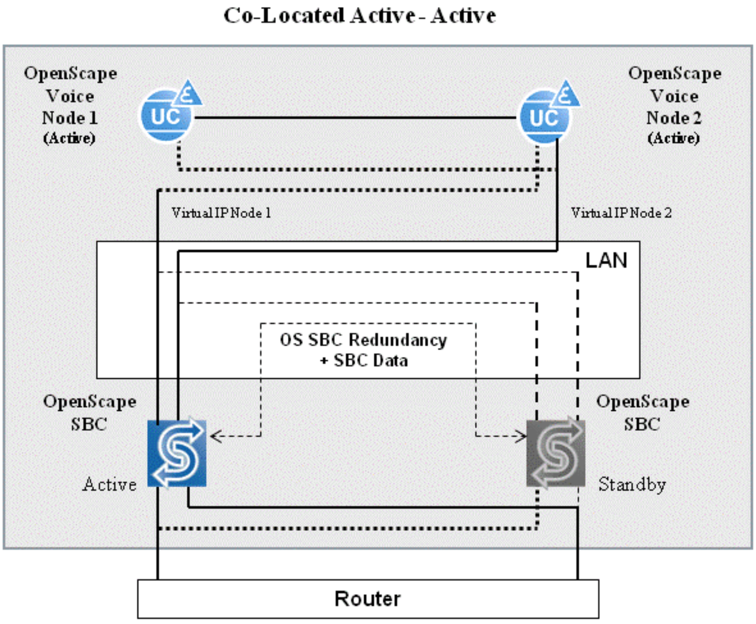
Simplex OpenScape Voice (OSV)



The OpenScape SBC does not require any special functionality to interface with a simplex OpenScape Voice (OSV). All SIP requests and responses are received at a single outside/ WAN interface of the OpenScape SBC and are relayed to a single OSV IP address. The OpenScape SBC is configured with Comm. System Type = Simplex.

An optional second OpenScape SBC can be used to provide a redundant SBC cluster if necessary although as OSV itself has no redundancy in this configuration.

Duplex co-located OpenScape Voice (OSV)


Co-Located Active - Active
OpenScape Voice Node 1 (Active)
OpenScape Voice Node 2 (Active)
UC
Virtual IP Node 1
Virtual IP Node 2
LAN
OS SBC Redundancy + SBC Data
OpenScape SBC
Active
OpenScape SBC
Standby
Router

When OpenScape Voice (OSV) is operating in duplex mode, end devices communicate with both nodes of the duplex OSV configuration, requiring the OS SBC cluster support 2 Virtual IP (VIP) addresses, one for each OSV node. For each OSV, an SBC inside VIP address associated with an outside VIP address is needed. Endpoint devices must be configured with one of the outside network VIP's as their SIP Server / SIP Registrar, distributed to provide a balance OSV load.

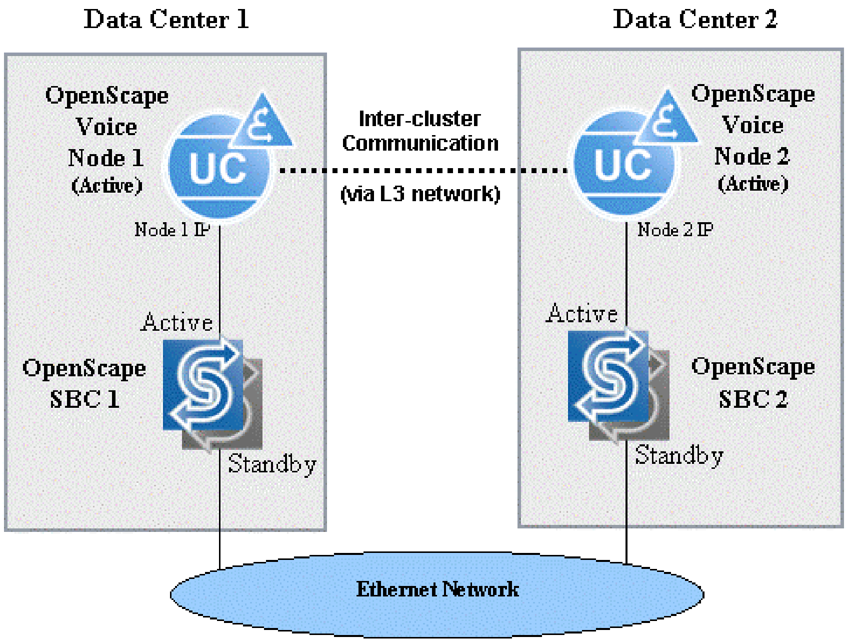
SBC redundancy is only available in an active-standby mode.

OS SBC node failover handling requires that both VIP address pairs (external and internal OSV bindings) are taken over or assumed by the OS SBC Standby Node.

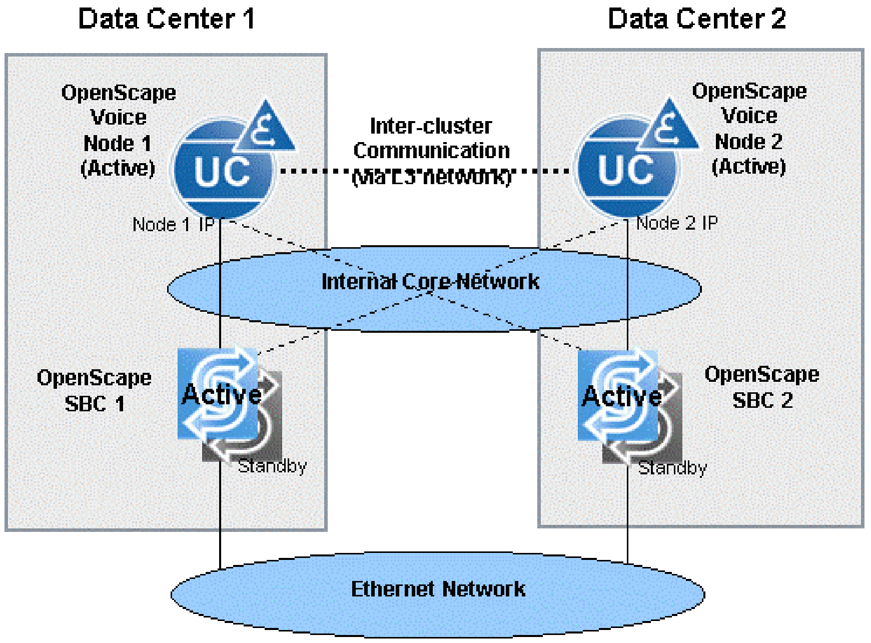
In this non-geographically separated configuration, OSV failures are transparent to the OS SBC since an OSV node failure leads to the partner OSV node taking over the internal VIP address of the failed OSV node assuming both inside network VIP addresses.

In the Active-Active OSV configuration, the OS SBC is configured with Comm. System Type = Collocated.

OpenScape Voice (OSV) L3 Geographically Separated Redundancy



OpenScape Voice Geographically Separated Redundancy (no internal core network)



OpenScape Voice Geographically Separated Redundancy (with internal core network)

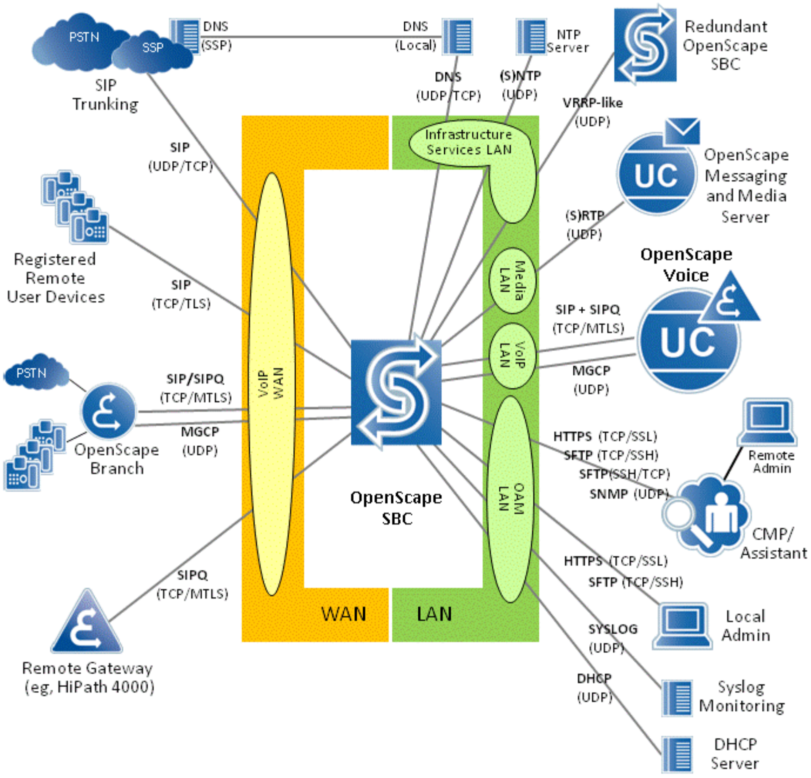
In addition to the OpenScape SBC redundancy on the same subnet for support of co-located OpenScape Voice redundant nodes, this feature provides support for OpenScape Voice redundancy of geographically separated nodes that are on separate subnets. A Layer 3 (L3) connection is used to exchange call state information between the geographically separated OpenScape SBCs.

At least two OpenScape SBC servers (one at each data center) are required to support OpenScape Voice geographically separated redundancy. Four OpenScape SBC servers are required (two at each data center) in case server redundancy at each data center is also required.

Unlike OpenScape SBC redundancy on the same subnet where a common set of SBC Session Licenses can be shared between the Active and Standby servers, OpenScape SBCs that are L3 geographically separated are counted as separate systems for purposes of SBC Session Licenses. In other words, a separate set of SBC Session Licenses need to be used for the OpenScape SBC system that are geographically separated.

Protocols

OpenScape SBC supports multiple protocols. The diagram below illustrates their usage in the network.



Security Certification

OpenScape SBC is rated Certified Secure by Miercom Independent Testing Labs. The Certified Secure rating is valid for a two-year period while advancements in both security countermeasures and vulnerability exploits continue to be monitored.

Certified Secure testing involves subjecting the product to a rigorous battery of vulnerability analyses and scans as well as a complex set of exploits designed by a team of experienced security professionals.

Miercom performed attacks as an outside attacker would, within the constraints of the test environment. The approach and methodology utilized in this test is based on knowledge that Miercom, in collaboration with leading security experts, has collected over several years through its work in VoIP pre- and post-deployment site surveys and security assessments, as it uses in testing other vendors SBC products.

1.4.1 Interworking

The OpenScape Session Border Controller (SBC) interworks with SIP endpoints, OpenScape Branches and SIP Service Providers.

Interworking with Other Equipment and Services

OpenScape SBC is compatible with and supports interoperability with all the SIP endpoint devices and versions supported by the OpenScape Solution Set.

OpenScape SBC is compatible with and supports interoperability with all OpenScape Branch models and version supported by the OpenScape Solution Set.

Most SIP Service Provider require certification with the customer’s VoIP equipment solution in order to order their SIP Trunk service and connect to their network. Please consult with Product Management prior to selling or deploying SIP Trunks before selling SIP Trunk service in any OpenScape solution.

1.4.2 OpenScape SBC Capacities

Dependent upon the OpenScape SBC server there is a maximum number of sessions, registered lines, trunks and traffic that can be supported.

Capacities and Performance

The capacity and performance of OpenScape SBC is dependent on the hardware server platform that is used. Capacity and performance values may vary based on several factors including the customer’s IP network configuration, SIP registration and keep-alive intervals, SIP session timer values, SIP signaling transport method, Digest Authentication usage, and SIP feature usage, particularly the usage of keyset operation and multiple contacts.

The values in the following table are provided based on the following configuration and operating characteristics, unless otherwise stated:

- SIP transport protocol (either of the following configurations):

    TLS for all connections; TLS keep-alive every 40 seconds and Digest Authentication disabled in the OpenScape Voice server

  Or

    TCP for all connections and Digest Authentication enabled in the OpenScape Voice server.
- SIP Session Timers enabled in OpenScape Voice server with the session expiration time set to 30 minutes.
- Default level logging enabled
- Average Call duration of 108 seconds

- Registration expiration time of 1 hour (on both sides of the SBC)
- No Keysets or Multiple Contacts

OpenScape SBC Capacity and Performance Values:

- Performance values are based on the Network interface switch speed set to 1 Gigabit Ethernet.

	IBM x3250 M3/ M5/M6 V7/V7R1 (note 1)	**IBM x3550 M3/ M4 / Fujitsu RX200 S6/S7 V7 (note 1)**	**IBM x3550 M3/ M4 /Fujitsu RX200 S6/S7 V7R1 (note 1)**
Max. allowed SIP registered lines/ users (note 2), (without Digest Authentication and without Throttling (note 3) or TLS)	6,000 (note 4)	20,000 (note 4)	50,000 (note 4)
Max. allowed SBC sessions (simultaneous SIP calls) (note 5)	1,200	4,000	8,000
Max. Simultaneous media streams anchored through OpenScape SBC (note 6)	600	2,000	8,000
Max. simultaneous SRTP secure media streams (either MIKEY0 or SDES) terminated/ mediated by SBC	480	1,600	6,400
Max. SIP Service Provider (SSP) Profiles	10	10	10
Number of Simultaneous SIP Service Providers	2	2	2
Average Call Holding time	80 s	80 s	180 s
Busy Hour Call Attempts (full-calls (note 7))	27,000	45,000	80,000

	IBM x3250 M3/ M5/M6 V7/V7R1 (note 1)	IBM x3550 M3/ M4 / Fujitsu RX200 S6/S7 V7 (note 1)	IBM x3550 M3/ M4 /Fujitsu RX200 S6/S7 V7R1 (note 1)
Maximum Peak half-calls per second (note 7), (without Digest Authentication and without Throttling (Note 3)	15 (note 8)	25 (note 8)	44 (note 8)
Registration refresh requests per second (randomized registration steady state condition)	5	16	26
Steady state call completion rate	99.99%	99.99%	99.99%
Time to recover to steady state (99.99% call completion) following simultaneous restart of all (6,000 or 20,000) subscriber devices (note 9)	<15 min.	<15 min.	<15 min.

NOTICE: 1 Network interface switch speed of hardware platforms is set to 1 Gigabit Ethernet.

NOTICE: 2 For keysets, each keyset line appearance is counted as one registered user.

NOTICE: 3 For a subscriber behind a NAT device, Throttling is a mechanism used to allow a NAT device to keep its pinhole open for the subscriber’s SIP signaling connection. In order to do this, a REGISTER coming from the subscriber is responded back with a small expiry interval (configurable, default 60 seconds) to force the subscriber to re-register often, which keeps the pinhole in the NAT device to remain open.

NOTICE: 4 Apply the following penalty (or penalties*) to determine the actual OpenScape SBC maximum registered users capacity limit when the following functions are enabled:

a: Digit Authentication penalty: 25%,

b: Throttling penalty** (600 seconds throttling interval): 60%, c: TLS penalty** (600 seconds keep alive interval; no throttling): 50%,

*: To determine cumulative penalties, apply penalty 1 and on the new number, apply penalty 2.

**: Throttling and TLS penalties are not applicable to hosted remote Branch users.

NOTICE: 5 An SBC Session is defined as a SIP signaling call with an access-side signaling leg and a core-side signaling leg. A typical voice call between a local openScape Voice user and a Remote User registered via the SBC, or to a SIP trunk connected via the SBC requires one SBC session. A typical video call requires two SBC sessions; one for the video connection and another for the audio connection. An additional 20% penalty on OpenScape SBC capacity should be added for a video connection versus an audio connection due to the extra SIP INFO messages that are exchanged during the video call.

NOTICE: 6 These are media streams routed through the SBC when a direct media connection between endpoints is not possible, for example, when the SBC needs to NAT the media packets because they reside in different subnets. Each "half-call" has two media streams traveling in the opposite direction.

For example, two "half-calls" are used when a remote user registered via the SBC is connected to another remote user registered via the SBC is connected to another remote user registered via the SBC, or to a SIP trunk connected via the SBC. A single "half-call" is used when a local subscriber registered directly with the OpenScape Voice server is connected to a remote user registered via the SBC, or to a SIP Trunk connected via the SBC.

NOTICE: 7 A “half call” is a call from either Access side (WAN) to Core side (LAN) or from Core side (LAN) to Access side (WAN). A “full call” consists of two "half call" legs, i.e. a call being initiated by the Access side (WAN) going to Core side (LAN) and then coming back to the Access side (WAN).

NOTICE: 8 Apply the following penalty (or penalties*) to determine the actual OpenScape SBC maximum registered calls per second limit when the following functions are enabled:

a: Digit Authentication penalty: 30%,

b: Throttling penalty** (600 seconds throttling interval): 40%,

c: TLS penalty** (600 seconds keep alive interval; no throttling): 50%,

*: To determine cumulative penalties, apply penalty 1 and on the new number, apply penalty 2.

**: Throttling and TLS penalties are not applicable to hosted remote Branch users.

NOTICE: 9 When restarting, SIP endpoint devices are required to comply with procedures specified in RFC3261 and OSCAR Chapter 11: Best Practices. With a simultaneous restart of all endpoint devices when a user becomes successfully registered, that user shall immediately be able to originate and receive calls with a call completion rate of at least 99.99%.

Capacity Calculation Example:

Based on the capacity data in the table it can be seen that an SBC session that requires the media stream be anchored uses twice as much SBC session capacity versus a call that does not require the media to be anchored. In addition, SRTP termination/mediation imposes another 25% penalty on the SBC session capacity versus a call with media anchoring that does not require SRTP termination/mediation.

Therefore, if there are 300 SBC sessions with the media anchoring and SRTP termination/mediation being applied, an equivalent of 750 (2 x 1.25 x 300 = 750) SBC sessions are consumed. If an IBM x3250 M3 server is being used, this would allow for 450 (1200 – 750 = 450) more SBC sessions that could be used for calls that do not require the media to be anchored before the total capacity of 1200 SBC sessions are consumed.

1.4.3 OpenScape SBC Sessions

Dependent upon the connection via the OpenScape Session Border Controller (SBC); one or more sessions may be required.

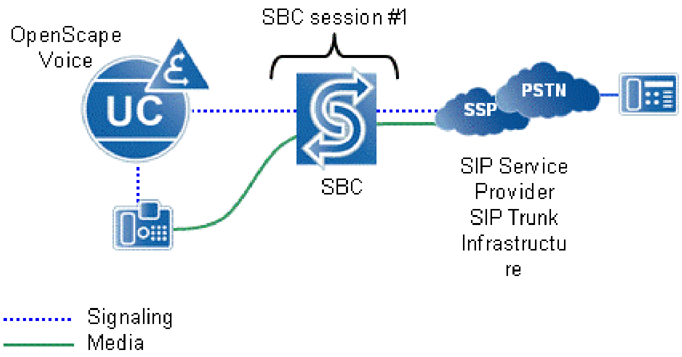
How OpenScape SBC Sessions are Counted

An OpenScape SBC Session License is consumed for each active SIP call connection that is being managed and processed by OpenScape SBC. Each SIP call connection may consist of the SIP signaling packets only (when media packets are being routed between the endpoints), or when both SIP signaling and media packets are being managed and processed by OpenScape SBC. In other words, if a SIP signaling connection traverses OpenScape SBC (that is, a SIP connection between the SBC core-side and the SBC access-side), with or without the corresponding media packets for that call, an SBC session is consumed.

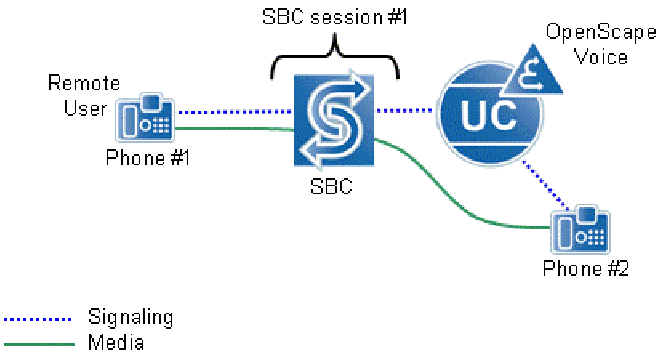
The figures below illustrate the following SBC session usage examples:

- **Example #1:** SIP Trunk call consuming one SBC session
- **Example #2:** Call between Remote User and Local user consuming one SBC session
- **Example #3:** Call between two Remote Users with media routed through SBC consuming two SBC sessions
- **Example #4:** Call between two Remote Users with media routed directly between phones consuming two SBC sessions

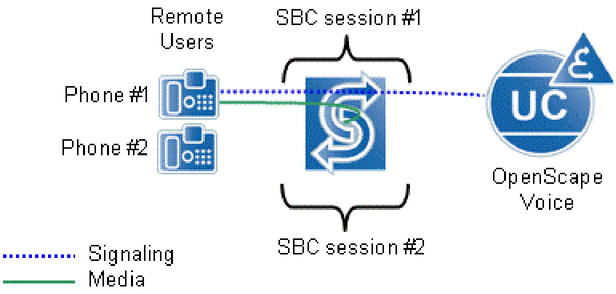
Example #1: SIP Trunking Call

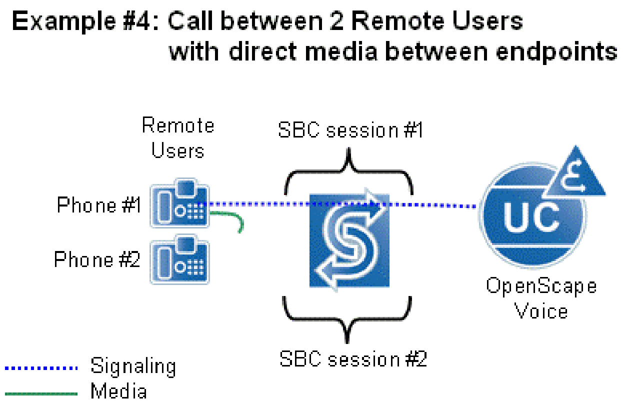


Example #2: Call between Remote User and Local User



Example #3: Call between 2 Remote Users
with media routed through SBC





1.4.4 Features

The OpenScape Session Border Controller (SBC) supports an abundance of features.

Feature List

For a quick identification of the supported features, the table below lists alphabetically sorted by name the available features.

Feature Name
Alarming
Alarms - Enhanced Alarm Information
Backup and Restore
Centralized SBC Functionality
CMP Integrated Management
DNS Support
Dynamic NAT device support at remote branches
Export/Import (configuration)
Firewall
Licensing
Licensing - Software Subscription Licensing (SSL)
Local Management
Logging
Media Anchoring
Media Pass-through
Multiple-device support behind Remote NAT Router
Near-end NAT Firewall Support
NTP Support

Feature Name
OpenScape Virtual Appliance
SBC Server Redundancy on the same Subnet (SBC Cluster)
SBC Redundancy support for L3 Geographical Separated OpenScape Voice Nodes
Secure calls to Microsoft Lync
Secure Management
Secure Software Download
Simplified Installation
SIP Message Inspection and Manipulation
Skype Connect Support
Smart Services Delivery Platform (SSDP)
SRTP Termination and Mediation
Subscriber Feature Support
Support of IBM x 3250 M3/M5/M6
Support of IBM x 3550 M3/M4
Support of Fujitsu RX200 S6/S7
TLS/SRTP
TLS Support for SIP Service Providers
Tracing
Traffic Control
Vitualization on VMware
VLAN support for connections to remote branch locations
Voice and Video Support
VPN

Features in OpenScape SBC

OpenScape SBC software includes the latest version features and features from prior releases.

Application Network Features

- **DNS Support** - OpenScape SBC supports the configuration of a route between the access network and the data center to facilitate DNS client access to a DNS server.
- **NTP Support** – OpenScape SBC supports the configuration to provide a local NTP or to synchronize to an external NTP server on the core side in order to provide NTP server function to the clients on the access.

Management, Administration and Serviceability Features

- **Alarms** – OpenScape SBC provides SNMP traps to the Assistant for alarm monitoring. It also supports a security log that captures events including logon success and failure, password changes, encryption failures, and configuration changes, that can be retrieved by secure remote login (ssh) or by real-time syslog event generation to a Syslog server, if configured.

- **Backup and Restore** – Upon download of a new software load OpenScape SBC supports automatic backup of the previous software load. The local management interface allows the Service Engineer to return to the previous software load if needed.

> **NOTICE:** Once the previous software load is restored, the new load is no longer available.

- **CMP Integrated Management** – OpenScape SBC supports integrated management via the Common Management Platform (CMP) together with the Assistant as for other OpenScape Solution network elements. The core-side LAN interface is used for management.
- **Export/Import Configuration** – OpenScape SBC supports export and import of configuration files within the CMP. Up to 100 configurations can be stored.
- **Licensing** – This feature provide support of the CAPEX and OPEX licensing models.
- **Licensing - Software Subscription Licensing (SSL) support** – OpenScape SBC supports a "pay-as-you-go” SSL licensing model whereby a customer is charged based on actual monthly usage of SBC session licenses instead of purchasing a large inventory of permanent licenses up front. With SSL the customer cost for the SBC is handled as a monthly operating expense (OPEX) instead of paying a large up front capital expense (CAPEX).
- **Local GUI capability to configure company name and product name** – Allows the capability to modify the company name and product to a customer provided name associated with the OpenScape SBC via the local OpenScape SBC Management tool. The name configured will appear on the OpenScape SBC local GUI.
- **Local Management** – OpenScape SBC supports an integrated local management interface using a web GUI.
- **Logging** – OpenScape SBC has the capability to collect Log data for all services and for RapidStat. It also supports a security log that captures events including logon success and failure, password changes, encryption failures, and configuration changes, that can be retrieved by secure remote login (ssh) or by real-time syslog event generation to a Syslog server, if configured.
- **OpenScape 4000 Operating Mode** – OpenScape SBC has an administration option that allows it to be configured for used with OpenScape 4000 systems in support of SIP trunking deployment scenarios. When used with OpenScape 4000, administration of the OpenScape SBC is preformed using its local administration interface, which is documented in the OpenScape SBC in the software release notes. Please refer to OpenScape 4000 product documentation for additional details
- **Simplified Installation** – This feature allows for alternate methods of installation to the OpenScape SBC with reduced installer on site interaction, including an option for “Simple” installation at customer site. CMP / Assistant is pre-configured to be able to recognize new OpenScape SBC and determine the proper s/w profile that should be used when the device is connected to the customer's network and announces itself to CMP / Assistant.

- **Smart Service Delivery Platform (SSDP)** – This feature provides a location on OpenScape SBC to support managed services based on the Smart Services Delivery Platform (SSDP), e.g., to provide information on products such as last restart date, CPU load, pulling software from a remote file server, etc. These data are sent real-time to the SSDP.
- **Tracing** – This feature adds the capability to OpenScape SBC to support continuous and on-demand tracing function to be used in conjunction with the OpenScape Voice Trace Manager.

System/Architectural Features

- **Centralized SBC Functionality** – OpenScape SBC is specifically designed to provide the functionality of a centralized SBC in the OpenScape solution environment. Although OpenScape SBC is required to be “logically” centralized it need not necessarily be in the same physical location as the other centralized OpenScape UC server(s), provided that the following requirements are satisfied and the associated restrictions are understood and accepted by the customer:

  1) OpenScape SBC’s core-side (LAN) interface must be on the same internal LAN to which the OpenScape Voice server(s) are connected. Be advised that there is no survivability for SIP trunks and endpoints that are connected via a remotely located OpenScape SBC when its LAN connection to the centralized OpenScape UC server(s) fails.

  2) The round-trip network delay between OpenScape SBC and the OpenScape Voice server must be less than 400ms. Greater network delays will trigger retransmission of SIP signaling messages which will negatively impact the SBC’s functionality and performance and when certain thresholds are exceed, cause OpenScape SBC to enter a mode where it will intentionally shut down its access-side (WAN) interface by design, causing remote users and branch offices to register to a alternate SIP server (eg, using DNS SRV) and cause SIP Service Providers to reroute SIP trunk calls to an alternate destination (eg, as a SIP trunk subscription option).

  > **NOTICE:** For OpenScape solutions that require non-centralized survivable SBC functionality, e.g., for support of SIP trunks at a branch office location, OpenScape Branch is the product that is designed for this purpose. Please refer to the OpenScape Branch Sales Information documentation for further information.

- **Media Anchoring** - OpenScape SBC supports the anchoring of media streams to be routed through the SBC when a direct media connection between endpoints is not possible. Media anchoring is necessary when NATing of media packets are required, for example, when the two connected endpoints reside in different IP network or subnets. A direct media connection between two connected endpoints is possible when NATing of the media packets is not required. In this case only the signaling connection needs to be routed via the OpenScape SBC and the media connection can be routed directly between the two endpoints.

  > **NOTICE:** When OpenScape SBC is connected to a remote OpenScape Branch office, the IP address assigned to the NAT device serving the remote branch office (eg, a DSL modem) must use a static IP address in order to facilitate

the proper operation of media anchoring and direct media connections. OpenScape SBC, Version 7 and later, supports the use of dynamic IP addresses on remote NAT devices.

- **Media Pass-through** - Media “pass-through” refers to OpenScape SBC handling of the media packet payload whereby the unencrypted RTP or encrypted SRTP media payload data that are received from the connected endpoints are relayed through the SBC without modification. With media pass-through, OpenScape SBC does not play a role in reformatting of the actual media payload so the media format, including negotiation of codec and encryption is performed between the media endpoints. This implementation allows for SRTP media encryption to be realized across the entire end-to-end path of the media connection, assuming that the connected endpoints support SRTP using a compatible key management protocol. Media packets are relayed through OpenScape SBC at near wire-speed when performing media pass-through.

- **Media Pass-through**- Media “pass-through” refers to OpenScape SBC handling of the media packet payload whereby the unencrypted RTP or encrypted SRTP media payload data that are received from the connected endpoints are relayed through the SBC without modification. With media pass-through, OpenScape SBC does not play a role in reformatting of the actual media payload so the media format, including negotiation of codec and encryption is performed between the media endpoints. This implementation allows for SRTP media encryption to be realized across the entire end-to-end path of the media connection, assuming that the connected endpoints support SRTP using a compatible key management protocol. Media packets are relayed through OpenScape SBC at near wire-speed when performing media pass-through.

- **Media Transcoding -** Effective with OpenScape SBC V8 Media Transcoding is supported between the OSV solution supported codecs G.711 (a-law, u-law), G.729 and G.722 and the iSAC and iLBC codecs of the WebRTC open-source project which shall be implemented in OSMO. The media transcoding mechanism makes use of the concept of administered Media Profiles.
- **Media Separation -**WAN interface separation of SIP signaling and Media for certain remote endpoint use cases, e.g. signaling is supported by private IP addresses (MPLS or VPN) while the media is supported in the public address space.
- **Multiple-device support behind Remote Nat Router** – In some configurations the OpenScape SBC can support only a single device or branch proxy behind a remote NAT router. Multiple subscribers behind a remote NAT router is possible provided the router meets certain requirements as described below:
  - NAT device must support NAPT (Network Address and Port Translation)
  - NAT device must support unique port mapping across different devices
  - If there is no port mapping established and NAT device receives any packets it should not put the originator in the blacklist but instead silently drop the packets. Once the port mapping is created by the device behind NAT then NAT device must start redirecting the packets to the device.
  - To additionally safeguard against having multiple devices behind NAT using the same port numbers, all devices should use TCP transport and unique RTP port numbers.
  - SIP ALG must be disabled in the NAT
  - The private IP addresses allocated to remote endpoints must be unique across all the endpoints.

  - TLS subscribers behind NAT must have connectivity check enabled to keep the NAT pin-hole open. For UDP and TCP subscribers, OS-SBC would use the REGISTER throttling to keep the NAT pin-hole open.
  - If the same NAT device is serving more than one internal networks with the overlap IP addresses, then it must expose the internal networks as a separate external IP address to the outside.

  Issues with supporting multiple devices behind a remote NAT router is usually only encountered with older NAT routers. Most all newer routers support the above requirements so it is seldom a problem with the newer NAT routers.

- **Near-End NAT Firewall Support** - This feature allows OpenScape SBC to operate in the customer's DMZ behind a data firewall that is performing Network Address Translation (NAT), which is also referred to as a near-end NAT. The external IP address of the near-end NAT (rather than OpenScape SBC's access-side IP address) becomes the basis for populating SIP messages and SDP sent to remote endpoints.
- **SBC Server Redundancy on the same Subnet (SBC Cluster)** - This capability allows the redundancy of an OpenScape SBC server by having a second server located on the same subnet having exactly the same database, thereby forming what is also known as an SBC cluster. A communications channel that is based on Virtual Router Redundancy Protocol (VRRP-like) is used between the SBC servers to keep call state information synchronized between the active and standby SBC servers, in order to provide failover with minimal impact on active calls. Some calls may be lost depending on the timing of the failover relative to the calls SIP signaling activity, particularly when a connection oriented protocol (TCP or TLS) is used for the SIP signaling transport.

  OpenScape SBC sessions are shared between the active/standby OpenScape SBC redundant server pair, so the number of SBC session required for a given call scenario is the same for an OpenScape SBC single server configuration as it is for an OpenScape SBC redundant server pair configuration.

  OpenScape SBC server redundancy on the same subnet can be deployed with an OpenScape Voice simplex system, or with an OpenScape Voice duplex system in which the OSV nodes are either a) co-located, in which case both OpenScape SBC redundant servers are also co-located, or b) geographically separated in two locations on the same L2 subnet, in which case the OpenScape SBC redundant servers can also be separately located in the same two locations as the OpenScape Voice nodes. The round-trip network delay of the VRRP-like connection between the redundant OpenScape SBC servers must be less than 100ms.

  The same type of HW server platform must be used for the two OpenScape SBC servers that comprise an SBC redundant pair.

- **SBC Redundancy Support for L3 geographically separated OpenScape Voice Nodes** – In addition to the OpenScape SBC redundancy on the same subnet for support of co-located OpenScape Voice redundant nodes, this feature provides support for OpenScape Voice redundancy of geographically separated nodes that are on separate subnets.

  - At least two OpenScape SBC servers (one at each data center) are required to support OpenScape Voice geographically separated redundancy. Four OpenScape SBC servers are required (two at each data center) in case server redundancy at each data center is also required.

  - Unlike OpenScape SBC redundancy on the same subnet where a common set of SBC Session Licenses can be shared between the Active and Standby servers, OpenScape SBCs that are L3 geographically separated are both active and running independent of each other, and are therefore counted as separate systems for purposes of SBC Session Licenses. In other words, a separate set of SBC Session Licenses need to be used for the OpenScape SBC system that are geographically separated. Furthermore, both OpenScape SBC clusters should be licensed with enough SBC Session Licenses to be able to handle the entire SBC traffic load in case the connection to one of the OpenScape SBC cluster is lost or one of the OpenScape SBC cluster (i.e., both OpenScape SBC servers of a redundant server pair) fails.
  - When used in a geographically separated OpenScape Voice configuration, remote SIP devices use DNS SRV to register to one of the OpenScape SBC clusters at one of the two data centers. The OpenScape SBC cluster that each SIP service is normally registered to is based on the SRV priority list so load balancing is possible. The registration will be refreshed by the SIP device until either the connection to its primary OpenScape SBC cluster is lost or its primary OpenScape SBC cluster (i.e.,both OpenScape SBC servers of a redundant server pair) fails. Should this happen, active calls will be dropped and the SIP device will register to the OpenScape SBC cluster at the other data center assuming it is active and accessible. TCP and UDP devices will get registered to the other OpenScape SBC cluster when they attempt to place a new call or upon expiry of the registration timer, whichever occurs first. Since it is not possible for OSV to deliver a call to the SIP device until it gets registered to the other OpenScape SBC cluster, a short period for the registration timer is recommended. TLS devices will get registered to the other OpenScape SBC within a maximum of 10 seconds due the TLS connectivity check that should be configured on the device. All normal call operation will resume once the SIP device gets registered to the OpenScape SBC cluster at the other data center.

- **Support for SBC Additional Deployment Scenarios** – The following additional OpenScape SBC deployment scenarios are supported with OpenScape SBC:
  - **Remote OpenScape Branch (SBC mode)**
  - **Remote Standalone SIP-Q Gateway**
  - **MGCP Signaling support for Remote Media Server**
  - **OpenScape Virtual Appliance**

    The OpenScape Virtual Appliance (Vapp) application allows ease of deployment of OpenScape Voice servers and applications including OpenScape SBC. Application functions include creation of the customer environment, distribution of software images and deployment of configuration data, installation files and licensing. In addition, provides the capability for mass provisioning.
  - **VLAN support for connections to remote branch locations**

    This feature provides support of multiple VLANs for connectivity to remote branches in customer networks where VLAN tagging is used to achieve network segmentation. In such networks, VLANs are used to differentiate between multiple remote branch locations that use overlapping private IP addresses.

    Each remote branch office is free to utilize overlapping IP address space with this feature; however, in addition to having a unique VLAN tag, a unique IP Address must be used by each remote branch office to communicate with OpenScape SBC’s access-side (WAN) interface. In a pure VLAN implementation this restriction would not exist as each remote branch office would be able to use the same IP address to communicate with the centralized SBC. OpenScape SBC’s access-side interface is supported on a single physical Ethernet interface without internal support of creating "sub-interface" bindings based on a VLAN tag. This is why it is necessary to assign a unique IP address for each unique VLAN.

- **SIP Header Inspection and Manipulation** – This feature is used to detect and manage incompatibilities that may exist between OpenScape solution and another system or network, such as a SIP Service Provider. It can insert headers that are expected by one side but not sent by the other, or to remove headers that one side cannot handle or to modify very granular contents of a header. The SIP header inspection and manipulation that is supported by OpenScape SBC is specifically designed to handle all of the call flows that may be encountered in an OpenScape solution. OpenScape SBC also supports configurable parameters necessary to support the various SIP header requirements that are necessary to interwork with a variety of SIP service providers.

  Other independent SBC vendors typically support customizable Header Manipulation Rules (HMRs) in order to accommodate all of the various carrier and enterprise environments in which their SBCs are used. Support for customizable HMRs are not necessary in OpenScape SBC since it is purpose built for use in the OpenScape solution, thereby making administration of the OpenScape SBC much easier than other SBC alternatives.
- **Skype Connect Support** – OpenScape SBC provides support for the unique SIP trunking requirements of the Skype Connect SIP trunking service related to IP-PBX authentication, account information and linkage to one or more identities which may be associated to IP-PBX business departments or users.

  OpenScape Voice solution components do not support the proprietary Skype video codec, for example:

  – Skype SIP trunking can be used to provide end-to-end video connectivity between compatible OpenScape video clients, eg, the Personal Edition (PE) and Enterprise Web Embedded (WE) clients.
  – A video connection between an OpenScape video client (eg, PE or WE client) and a Skype’s PC video client (eg, a Skype user on the Internet) is not supported.
  – Refer also to OpenScape Video Sales Information documentation for use of OpenScape SBC in the video solution.
- **Support of IBM x3250 M3** – The OpenScape SBC is supported on the IBM x3250 M3 platform.
- **Support of IBM x3250 M5** – The OpenScape SBC is supported on the IBM x3250 M5 platform.
- **Support of IBM x3250 M6** – The OpenScape SBC is supported on the IBM x3250 M6 platform.
- **Support of IBM x3550 M3** – The OpenScape SBC is supported on the IBM x3550 M3 platform.
- **Support of IBM x3550 M4** – The OpenScape SBC is supported on the IBM x3550 M4 platform.
- **Support of Fujitsu RX200 S6** – The OpenScape SBC is supported on the Fujitsu RX200 S6 platform.

- **Support of Fujitsu RX200 S7** – The OpenScape SBC is supported on the Fujitsu RX200 S7 platform.
- **Traffic Control** - OpenScape SBC assures Quality of Service (QoS) by supporting Differentiated Services Code Point (DSCP) settings for different traffic types like Signaling, Media and Management traffic. The DSCP settings can be configured down to the port level.

> **NOTICE:** Note: OpenScape SBC does not support QoS data collection.

- **Virtualization on VMware** - OpenScape SBC allows for deployment in a customer's virtualized environment together with other OpenScape Solution Set components, using VMware ESX/ESXi technology

  When virtualized, the OpenScape SBC application and its required operating system can run on a hardware-independent platform on top of a virtualization layer. The virtualization layer enables multiple applications, including applications that require different operating systems, to run simultaneously on the same server. VMware ESXi's vSphere client provides the interface to vCenter and the server where the OpenScape SBC virtual machine is running, and also provide support of vMotion, VMware Snapshot, and VMware HA (high availability) for the virtualized OpenScape SBC.

  Virtualization of OpenScape SBC is supported on vSphere V4.1/V5/V6/V6.5.

OpenScape Solution Endpoint Devices and Subscriber Features

- **Subscriber Feature Support** – OpenScape SBC supports all subscriber features of the OpenScape Solution Set for calls that are connected to the OpenScape Voice server via OpenScape SBC.
- **Voice and Video Support** – OpenScape SBC supports both voice and video connections for the subscriber endpoint devices that comprise the OpenScape Solution Set, for example voice devices such as OpenStage phones and video clients such as the Personal Edition (PE) and Enterprise Web Embedded (WE) clients.

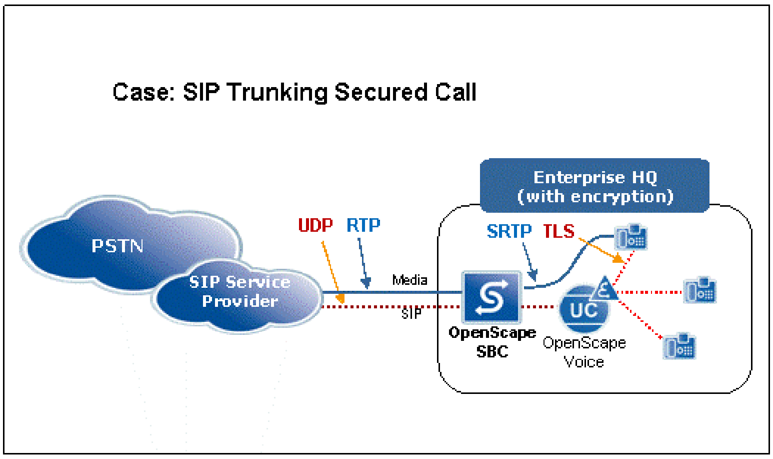
Security Features

- **Firewall** – OpenScape SBC provides an internal firewall for securing the communication and performs stateful Network Address Translation / Port Address Translation (NAT/PAT) inspection. It supports intrusion detection, Strict TCP Validation to ensure TCP session state enforcement, validation of sequence and acknowledgement numbers, rejection of bad TCP flag combinations.
- **Secure calls to Microsoft Lync** – This feature supports interworking between Microsoft Lync's SRTP/SDES implementation (single m-line) and SEN's best effort SRTP/SDES implementation (dual m-line), to allow SRTP media encryption between the two environments.
- **Secure Management** – OpenScape SBC provides secure access and file transfer via the use of Secure Shell (SSH).
- **Secure Software Download** – OpenScape SBC supports secure software download via SFTP.
- **SRTP Termination & Mediation (for MIKEY0 and SDES)** – OpenScape SBC provides support for SRTP MIKEY0 and SRTP SDES termination and mediation, which allows it to perform SRTP to RTP interworking and also

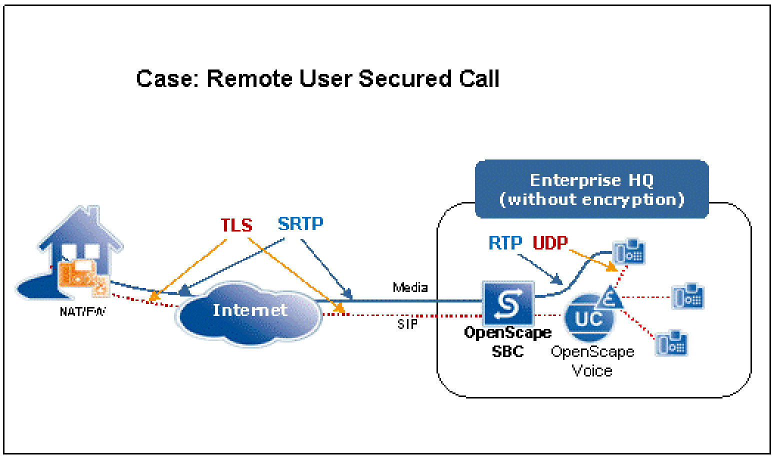
SRTP mediation between MIKEY0 and SDES key exchange methods for media connections that are routed via the SBC.

This feature is useful, for example, to maintain maximum media stream security within the enterprise network when using SIP trunks to a SIP service provider that does not support SRTP, or to ensure security for Remote Users (e.g., home workers) that access OpenScape Voice via the Internet. Please note that termination of the SRTP media stream that is necessary for the SBC to perform this mediation function significantly reduces the maximum concurrent session capacity of the SBC.

SIP Trunking Secured Call (below): SIP Trunk Secured Call with maximum media stream security within the enterprise network when using a SIP Trunk to a SIP service provider that does not use SRTP.



Remote User Secured Call (below): Remote User Secured Call to ensure security for Remote Users (e.g., home workers) that access OpenScape Voice via the Internet.



OpenScape SBC supports a configurable option for media handling for each location domain/endpoint that can be set to 1) pass-through, RTP, or SRTP. Calls between endpoints that are both set for pass-through will negotiate media security on an end-to-end basis between the endpoints without SBC termination or mediation. For calls to/from an endpoint configured for RTP or SRTP, the SBC will dynamically determine if the secure connection can be established to the partner endpoint using pass-through (ie, when the partner endpoint is also configured the same, either for RTP or for SRTP with a compatible MIKEY0 or SDES key management protocol), or if the SBC needs to provide SRTP termination (ie, when the partner endpoint is configured for RTP), or if the SBC needs to provide SRTP mediation between MIKEY0 and SDES when the partner endpoint is configured for SRTP but with a different key management protocol.

- **TLS Support for SIP Service Providers** - This feature enables OpenScape SBC to establish a secure session to a SIP Service Provider in order to encrypt the SIP signaling using TLS or MTLS (mutual TLS). TLS/MTLS is required for the secure signaling connection so that the keys which are negotiated for SRTP are not exchanged in clear. This feature also enables configuration of certificates on a per SIP Service Provider basis and provides improved certificate validation.
- **TLS/SRTP** – This feature allows OpenScape SBC to support secure calls by the usage of TLS (Transport Layer Security) encrypted signaling and SRTP (Secure Real-Time Transport Protocol) encrypted media traffic for communication. OpenScape SBC supports SRTP for both pass-through and termination/mediation scenarios.

  OpenScape SBC supports the following crypto suites for interoperability with the other solution components of the OpenScape UC Suite:

  Encrypted Signaling: TLS_RSA_WITH_AES_128_CBC_SHA

  Encrypted Media: AES_CM_128_HMAC_SHA1_80
- **VPN** – OpenScape SBC supports a single Virtual Private Network (VPN) connection based on IPSec and key generation based on OpenSSL. Supported message digest are MD2, MD5, MDC2 , RMD-160, SHA, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. Supported encoding and Cipher are: Base64 Encoding, Blowfish, CAST, CAST5, DES, Triple-DES, IDEA, RC2, RC4, RC5. If use of multiple VPNs is required, since OpenScape SBC supports only a single VPN connection, a VPN concentrator must be used on the access side of the OpenScape SBC.

1.4.5 Countries and Languages

An abundance of countries and languages are supported by the OpenScape Session Border Controller (SBC).

Availability of Countries

OpenScape SBC is available to all OpenScape Voice countries. Availability of OpenScape SBC in each country is contingent on the generic certifications of the hardware server platforms like UL, FCC and CE, and as some countries have some country specific certification such as Anatel for Brazil, CCC for China, VCCI for Japan, and others.

There are different hardware server platforms offered with OpenScape SBC based on IBM and Fujitsu servers, and these vendors already have certified their servers in many countries that require additional certifications.

Please note that country specific certifications are on-going and therefore subject to change. Also be advised that OpenScape SBC is available only in countries in which the OpenScape Solution Set is available and therefore may not be available in all countries. Please verify with the Sales Representative for the latest availability.

Languages

Various languages are supported for the Common Management Platform (CMP) /Assistant and the Local Management Portal.

The Management of the OpenScape SBC is available in the following languages:

- Common Management Platform (CMP) / Assistant

  English

  German

- Web based local GUI

  English

- OpenScape SBC Installation and Upgrades, Installation Guide

  English

  German

- OpenScape SBC Administration Documentation

  English

  German

- OpenScape SBC Data Sheet

  English

  German

2 General Installation - Overview

This chapter describes the options for installing software and hardware for OpenScape SBCs.

OpenScape SBC Assistant Configuration

"General Settings" is used to configure a secure method of transport between OpenScape SBC Assistant and the OpenScape Voice Assistant for the purpose of transferring files.

Installation Options

There are two types of installation procedures: “Simplified Installation” and “Basic Installation”.

Simplified Installation provides four options:

- **Option 1 (LAN MAC Address):**

  The OpenScape server hardware is pre-loaded with the required installation software prior to shipping to the customer. The installation does not require a USB stick. The LAN MAC address is pre-configured in the OpenScape SBC Assistant and is used to communicate from the OpenScape hardware to the OpenScape SBC Assistant to fetch software and configuration data.

  DHCP servers are used to communicate the pre-configured Common Management Platform (CMP) URL to the OpenScape server hardware. DHCP also provides a temporary IP address to the OpenScape server to be used during the download process. The OpenScape SBC Assistant must be configured with the software load required for this particular server.

  NOTICE: The OpenScape SBC is configured to run on the first network interface (LAN interface) and will accept the first DHCP Offer that contains Option 43 with a CMP FQDN or IP Address. If on the first network interface (LAN) a DHCP Offer is not returned or is returned but does not contain Option 43, then the OpenScape SBC will send a DHCP Discover message out the second network interface (WAN interface) if configured. If that DHCP offer contains Option 43 with a CMP FQDN or IP Address, the OpenScape SBC will then accept that DHCP Offer from the second network interface (WAN) and use that interface to contact the CMP. The OpenScape SBC ignores any DHCP Offers which do not contain Option 43.

- **Option 2 (Local Logical ID):**

  The OpenScape SBC server hardware requires a USB stick for installation. The USB stick is pre-loaded with required installation software including the Logical ID information for the OpenScape SBC prior to shipping to the customer. The Logical ID information is comprised of <name of the OpenScape Voice connected to> : <business group name> : <branch

name> and is used to communicate from the OpenScape hardware to the OpenScape SBC Assistant to fetch software and configuration data.

DHCP servers are used to provide the temporary IP address, as well as, to communicate the pre-configured Common Management Platform (CMP) URL to the OpenScape server hardware.

The OpenScape SBC Assistant must be configured with the software load required for this particular server.

- **Option 3 (Local CMP URL)**:

  The OpenScape SBC server hardware requires a USB stick for installation. The USB stick is pre-loaded with required installation software including the Logical ID information for the OpenScape SBC and the CMP URL prior to shipping to the customer.

  Pre-configuration of the DHCP servers is required when using this option. A temporary dynamic IP is set up for communication between the DHCP server and the OpenScape hardware.

  The OpenScape SBC Assistant must be configured with the software load required for this particular server.

- **Option 4 (Local xml Config File)**:

  The OpenScape SBC server hardware requires a USB stick for installation. The USB stick is pre-loaded with required installation software including and a xml configuration file for the OpenScape SBC prior to shipping to the customer. The xml file contains the Logical ID, Static IP address and address of the CMP to be used.

  Pre-configuration of the DHCP servers is not required when using this option. The Static IP is used to communicate between the CMP and the OpenScape hardware.

Basic Installation:

The OpenScape SBC “Basic Installation” is the pre-Version 2 OpenScape SBC installation method. Installation requires the use of a memory stick with the current software load and the assigned IP address for the system.

Refer to the **OpenScape SBC Hardware - Overview** chapter for detailed installation steps.

2.1 OpenScape SBC Assistant - Configuration

This chapter describes configuration for the OpenScape SBC Assistant.

General Settings

The "General Settings" option is used to configure a secure method of transport between OpenScape SBC Assistant and the OpenScape Voice Assistant for the purpose of transferring configuration.

2.1.1 How to Configure OpenScape SBC Assistant - General Settings

Proceed as follows to configure OpenScape SBC Assistant General Settings:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **General Settings** in the Navigation Tree under Administration.

   The system presents the **General Settings** dialog.
3) Proceed as follows to enable secure transport between the OpenScape SBC Assistant and the OpenScape Voice Assistant:
   a) Check the **Secure transfer** checkbox.
   b) The **Security transfer** checkbox indicates the enables secure communications via SOAP between the OpenScape SBC Assistant and the OpenScape Voice Assistant. When “unsecured” (unchecked) the transport method is unsecure via HTTPS.

      NOTICE: The following transport mechanism is used to transfer files from the OpenScape SBC Assistant (certain files only apply to OpenScape SBC servers).

      - - Software Load: HTTPS only
      - - Configuration File: HTTPS or SOAP (Secure

      NOTICE: If the Transport mechanism is set to **Secure transfer** and the OpenScape Branch or OpenScape SBC load does not support the new SOAP transport method, OpenScape Branch or OpenScape SBC is booted with the newest software load and apply the default Configuration file. An alarm is generated to indicate that file transfer has failed due to the wrong transport mechanism.
   c) Click the **Save** key to complete configuration.

   When the Secure transfer is enabled, from that point the OpenScape SBC Assistant will communicate securely to the OpenScape Voice Assistant.

2.2 Simplified Installation Steps

This chapter describes the general steps for OpenScape SBC simplified installation of software and hardware.

General Steps Checklist

The following is a checklist of general steps. Some steps may only apply to certain installation options as indicated.

1) **Download Installation Files Into the CMP:**

Download all installation files to the Common Management Platform (CMP). Installation files include:

Mandatory files:

- SPA file
- Software load image
- Configuration file (XML file)

Optional files:

The downloaded files are used to install multiple OpenScape SBC servers.

- Required for Option 1-4

2) **Pre-configure the DHCP Server:**

Pre-configure the URL associated with the Common Management Platform (CMP) into the DHCP server.

- Required for Option 1-2

The DHCP server must return a “temporary” IP address to be used for downloading the OpenScape SBC server.

- Required for Option 1-3

NOTICE: OpenScape SBC during DHCP server discovery sends out a DHCP Discover message with Option 60 Vendor Class Identifier automatically set to "OpenScapeSBC" (without the quotes).

NOTICE: The DHCP Server must be configured to contain the matching Vendor Class Identifier Option 60 so that the associated Option 43 parameters specific to this vendor class can be provided to the OpenScape SBC from the DHCP Server. The Option 43 parameters returned to the OpenScape SBC in a DHCP Offer will include the Common Management Platform FQDN(s) or IP Address(es) so that the OpenScape SBC can contact it to authenticate and download the necessary files to begin the installation procedure. In order to provide the correct Option 43 Vendor Specific Information to the OpenScape SBC in a DHCP Offer, the DHCP Server must not only be provisioned with Option 60, but also be provisioned with Option 43 containing the Common Management Platform FQDN(s) or IP Address(es).

3) **Add the OpenScape Session Border Controller (SBC) to OpenScape Voice Assistant:**

Add the OpenScape SBC into the Common Management Platform (CMP), OpenScape Voice Assistant.

- Required for Option 1-4

4) **Add the OpenScape Session Border Controller (SBC) to OpenScape SBC Assistant:**

Add the OpenScape SBC into the Common Management Platform (CMP), OpenScape SBC Assistant. The OpenScape SBC will automatically appear in the OpenScape SBC Assistant when configured in the OpenScape Voice Assistant and does not need to be manually added.

- Required for Option 1-4

5) **Configure the Software Load and Hardware Type for the OpenScape SBC:**

Configure the Software Load to be downloaded to the server and the Hardware Type of the server for the OpenScape SBC in the Common Management Platform (CMP), OpenScape SBC Assistant.

> **NOTICE:** If desired, the full configuration associated with each device, may also be downloaded to the CMP. If this is done, the download will include the “config.xml” file and the device will boot up with this configuration database.

- Required for Options 1-4

6) **Configure the Data Configuration File for the OpenScape SBC:**

A Data configuration file can be downloaded to the OpenScape SBC using the Common Management Platform (CMP), OpenScape SBC Assistant.

- Optional for Options 1-4

7) **Add the LAN MAC Address to the OpenScape SBC Assistant:**

Add the OpenScape SBC into the Common Management Platform (CMP), OpenScape SBC Assistant.

- Required for Option 1 only

8) **Connect the OpenScape Hardware to the Network:**

Install the OpenScape server onto the network. Plug in the USB stick into the OpenScape SBC server and power up the server. Upon power up installation information is exchanged between the CMP and the OpenScape SBC server. The list of installation files includes the software load, configuration file and possibly media files and config.xml file for the database. The device may boot up to three times during the process of downloading and installation.

- USB stick not required for Option 1
- USB stick required for Option 2-4

> **NOTICE:** OpenScape SBC Access to CMP (unsecured port 4709) must be configured in the OpenScape SBC Assistant prior to powering up the server. This is required to allow authentication, configuration and licensing information.

9) **Troubleshooting Installation Errors and Alarming:**

The OpenScape SBC server will log errors and produce alarms when possible, if errors occur during installation. Resolve errors and re-install.

10) **Confirmation Installation is complete:**

The OpenScape SBC Assistant can be used to view the status of all the OpenScape SBC devices as they are being installed. The status will indicate the current state of the installation process including if the OpenScape SBC device was successfully installed, the failure state, and reason (when provided). Once an OpenScape SBC device has been successfully installed the state shown in the OpenScape SBC Assistant will be “normal”.

Should the OpenScape SBC software need additional updates, the normal OpenScape SBC Batch processing functions can be used.

The OpenScape SBC server will signal that installation is complete by audible alert. Audible alarm as are also used to signal installation issues.

2.2.1 How to Download Installation Files Into the CMP

Proceed as follows to install files to the repository to the Common Management Platform (CMP). The downloaded files include product software loads and can be used to install multiple OpenScape SBC servers.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Maintenance** > **Inventory** within the Navigation Bar in the Common Management Platform.

The system presents the **Nodes & Application** Navigation Tree.

2) Select **Repository** from the Navigation tree.

The **Software Repository** window appears with a list of software.

> **NOTICE:** Note that effective with OpenScape SBC V8 the software versions use the’Fit4more’ format. For example,
>
> 08.00.03.00-2 (V8 R0.3.0)
>
> 08.00.04.00-1 (V8 R8.4.0)

3) Click the **Add...** button, in the work area navigation bar.

The **Add to software repository** window appears.

4) Select the **Browse...** button to search and select a file. One to ten files can be downloaded at one time. These files can be individual files or zip files. It is required to download the SPA file and software image.tar file for software updates.

> **NOTICE:** The SPA file for software update which contains the meta information **must be the first file** in the download list.

The **browser** window appears, for search and selection of a file.

5) Select the file from the browser and **Open** to add the file to the list to be loaded.

The **Add to software repository** window is updated with the selected file information.

6) Click the **Add** button next to **Add another file** to add additional files when greater than 10 files are required.

The **Add to software repository** window appears.

7) Click the **Save** button to update the CMP software repository.

The **Add software repository** window closes and the Software repository window appears with the updated software file information.

> **NOTICE:** Configuration files must be transferred manually to CMP in the following directories:

- **Offboard** (separate server used for CMP):

  Configuration File directory:

  ```
  /opt/siemens/openbranch/ob_config/<Logical_ID>/
  Configuration_File
  ```
- **Onboard** (aka Integrated, CMP runs in the same OpenScape Voice server):

  Configuration File directory:

  ```
  /img/enterpriseimg/primary/openbranch/ob_config/
  Configuration_File
  ```

8) The CMP repository now has the required installation software.

The software in the CMP repository can now be used to install multiple OpenScape severs.

2.2.2 How to Configure a Windows DHCP Servers

OpenScape device DHCP client will Broadcast a DHCP discovery Request with Option 60 Vendor Class Identifier automatically set to "OpenScapeSBC". The DHCP Server shall acknowledge with information via Option 43 containing the Common Management Platform FQDN(s) or IP Address(es). Proceed as follows to configure a Windows DHCP server with Common Management Platform (CMP) information used for Simplified Installation Options 1-2:

Prerequisites

Adequate administrative permissions.

DHCP Servers are available to the OpenScape devices in the customers network and used for temporary Dynamic IP address retrieval.

Step by Step

1) Configure Option 60: Enter the following information into the DHCP server.

a) Open the DHCP Console in Windows Server 2003/2008

b) Select (highlight) the DHCP Server in the navigation tree, right click on it and select **Define Vendor Classes**.

The **DHCP Vendor Classes** window appears.

c) Click the **Add** button.

The **New Class** window appears.

d) Enter the following Vendor Class Information: **Display Name** e.g., OSBC_VCI, **Descriptione**.g., OpenScape SBC Vendor Class Identifier.

e) Click the field under the **ASCII** column in the table and enter the value “OpenScapeSBC” (without quotes) in the field.

f) Click the **OK** button when finished.

The **New Class** window closes and the **DHCP Vendor Classes** window appears with the new vendor class displayed.

g) Click the **Close** button.

Option 60 is configured.

2) Configure Option 43: Enter the following information into the DHCP server.

a) Open the DHCP Console in Windows Server 2003/2008 (may be currently opened)

b) Select (highlight) the DHCP Server in the navigation tree, right click on it and select **Predefine Options**.

The **Predefined Options and Values** window appears.

c) Select the option class previously created (OSBC_VCI) from the **Option class** field list.

The **Add** button becomes active.

d) Click the **Add** button.

The **Option Type** window appears.

e) Enter the option type name in the **Name** field e.g., OSBC-Opt43-for-CMP.

f) Select data type **String** in the **Data type** field list.

g) Enter **1** for the code in the **Code** field. This will return Type 01 in Option 43 which the OpenScape SBC requires.

h) Enter description in the **Description** field (optional) e.g., OSBC Opt43 for CMP FQDN/IP.

i) Click the **OK** button when finished.

The **Option Type** window closes and the **Predefined Options and Values** window appears with the new Option name displayed.

j) Enter the IP Address of the Common Management Platform (CMP) in the **Value** field. This could also consist of a single FQDN if desired, two

FQDNs or two IP Addresses if CMP redundancy exists, which all can resolve to the Common Management Platform IP Addresses.

Example: String value is a single IP Address for CMP: 10.245.4.52

Example: String value contains two CMP IP Addresses: 10.245.4.52,10.245.4.62

Example: String value is a single FQDN for the CMP: cmp52.simpinst.com

Example: String value contains two FQDNs (comma separated): cmp52.simpinst.com,cmp52.simpinst.com62

k) Click the **OK** button.

Option 43 is configured and the **DHCP** main window appears.

3) Assign Option 43 to the DHCP Scope: Enter the following information into the DHCP server.

a) Open the DHCP Console in Windows Server 2003/2008 (may be currently opened)

b) Select (highlight) the DHCP Server in the navigation tree, right click on it and select **Configure Options**.

The **Scope Options** window appears.

c) Select the **Advanced** tab.

The **Advanced** work area appears.

d) Select the vendor class previously created (OSBC_VCI) from the **Vendor class** field list.

The **Available Options and Description** is populated in the table.

e) Checkmark the option previously created for Option 43 in the checkbox.

The **Data entry String value** is automatically updated with the CMP IP or FQDN information.

f) Click the **OK** button.

Option 43 is assigned and the **DHCP** main window appears.

4) Pre-configuration of the DHCP server is complete.

The OpenScape SBC is configured to run on the first network interface (LAN interface) and will accept the first DHCP Offer that contains Option 43 with a CMP FQDN or IP Address. If on the first network interface (LAN) a DHCP Offer is not returned or is returned but does not contain Option 43, then the OpenScape SBC will send a DHCP Discover message out the second network interface (WAN interface) if configured. If that DHCP offer contains Option 43 with a CMP FQDN or IP Address, the OpenScape SBC will then accept that DHCP Offer from the second network interface (WAN) and use that interface to contact the CMP. The OpenScape SBC ignores any DHCP Offers which do not contain Option 43.

After the DHCP server is configured additional simplified installation steps are required prior to installation of an OpenScape Session Border Controller.

2.2.3 How to Configure a LINUX DHCP Server

OpenScape device DHCP client will Broadcast a DHCP discovery Request with Option 60 Vendor Class Identifier automatically set to "OpenScapeSBC". The

DHCP Server shall acknowledge with information via Option 43 containing the Common Management Platform FQDN(s) or IP Address(es). Proceed as follows to configure a LINIUX DHCP server with Common Management Platform (CMP) information used for Simplified Installation Options 1-2:

Prerequisites

Adequate administrative permissions.

DHCP Servers are available to the OpenScape devices in the customers network and used for temporary Dynamic IP address retrieval.

Step by Step

1) The following details the specific configuration parameters that are required to provision a Linux DHCP Server for Simplified Installation with the OpenScape SBC. The parameters below refer to the specific settings needed for the Simplified Installation with the OpenScape SBC outside of the typical DHCP server settings already existing in the customer environment if using a Linux DHCP Server (DHCP Address Pools, Reservations, Default Gateway, DNS server addresses, etc. as this depends on the customer infrastructure)

a) Only the "option Vendor.swsupply1" line should be used and can be populated with either a single FQDN, a single IP Address, two FQDNs or two IP Addresses (separated by a comma) for representing CMP redundancy

The "option Vendor.swsupply2" (code 2) should not be used, as the OpenScape SBC only recognizes and accept Option 43 responses with Type Code 01. The "option Vendor.swsupply2" uses Type Code 02 which the OpenScape SBC does not accept for representing a CMP address

b) If the DHCP Discover message sent by the OpenScape SBC upon bootup contains Option 60 Vendor Class Identifier equal to the value "OpenScapeSBC", the DHCP Server will return in the DHCP Offer Option 43 with one of the values not commented out in "option Vendor.swsupply1" under the "Vendor" class.

c) In the example below, the DHCP Server will return in the DHCP Offer Option 43 with 10.234.3.35, which represents the Common Management Platform IP Address

Only one value in "option Vendor.swsupply1" can be active at a time within this dhcp.conf file. In the example below, having either of the "option Vendor.swsupply1" values active (not commented out) will return in Option 43 the associated entries (the first returns a single IP Address, the second returns a single FQDN, the third returns two IP Addresses (separated by a comma), and the fourth returns two FQDNs (separated by a comma)

Example data:

- the customer domain is simpinstall.com
- the customer is providing addresses via DHCP for network 10.20.1.0/24 GW: 10.20.1.1
- the customer's DHCP Scope is for addresses 10.20.1.10 thru 10.20.1.100
- the customer's two DNS Servers are 10.20.4.230 and 10.20.5.230

- the customer's CMP is at IP Address 10.234.3.35 based on "option Vendor.swsupply1”

DHCP Server settings in the /etc/dhcpd.conf file:

```
option domain-name "simpinstall.com";
option domain-name-servers 10.20.4.230, 10.20.5.230;
option routers 10.20.1.1;
#
class “Vendor” {
option Vendor.swsupply1 “10.234.3.35”;
# option Vendor.swsupply1 "cmp35.simpinstall.com";
# option Vendor.swsupply1 "10.234.3.35,10.234.2.206";
# option Vendor.swsupply1 "cmp35.simpinstall.com";
# option Vendor.swsupply1
 "cmp35.simpinstall.com,cmp36.simpinstall.com";
match if option vendor-class-identifier =
 “OpenScapeSBC”;
vendor-option-space Vendor:
}
subnet 10.20.1.0 netmask 255.255.255.0 {
range 10.20.1.10 10.20.1.100;
default-lease-time 86400;
max-lease-time 1800;
}
```

2) Pre-configuration of the DHCP server is complete.

The OpenScape SBC is configured to run on the first network interface (LAN interface) and will accept the first DHCP Offer that contains Option 43 with a CMP FQDN or IP Address. If on the first network interface (LAN) a DHCP Offer is not returned or is returned but does not contain Option 43, then the OpenScape SBC will send a DHCP Discover message out the second network interface (WAN interface) if configured. If that DHCP offer contains Option 43 with a CMP FQDN or IP Address, the OpenScape SBC will then accept that DHCP Offer from the second network interface (WAN) and use that interface to contact the CMP. The OpenScape SBC ignores any DHCP Offers which do not contain Option 43.

After the DHCP server is configured additional simplified installation steps are required prior to installation of an OpenScape Session Border Controller.

2.2.4 How to Configure a Cisco Router Utilizing the DHCP Server

OpenScape device DHCP client will Broadcast a DHCP discovery Request with Option 60 Vendor Class Identifier automatically set to "OpenScapeSBC". The DHCP Server shall acknowledge with information via Option 43 containing the Common Management Platform FQDN(s) or IP Address(es). Proceed as follows to configure a Cisco Router Utilizing the DHCP server with Common Management Platform (CMP) information used for Simplified Installation Options 1-2:

Prerequisites

Adequate administrative permissions.

DHCP Servers are available to the OpenScape devices in the customers network and used for temporary Dynamic IP address retrieval.

Step by Step

1) The steps needed to set up a Cisco Router to act as a DHCP Server can be obtained from the Cisco Web Site. The following provides the specific configuration parameters necessary for the Simplified Installation to work with the OpenScape SBC with a Cisco Router DHCP Server.
2) Configure Option 60: Enter the following information into the “ip dhcp pool”.
   - **option 60 hex 4f70.656e.5363.6170.6542.7261.6e63.68**

   NOTICE: in hex this string is equal to: OpenScapeSBC
3) Configure Option 43: Enter the following information into the “ip dhcp pool”.
   - Option 43 hex string is assembled by concatenating TLV values (Type + Length + Value)
   - For whatever string value is desired for the FQDN(s) or IP Address(s) for the Common Management Platform, the Option 43 must begin with the first byte being “01” for Type Code 01, the second byte representing the length in bytes of the actual value, followed by the representative string value bytes.

   Example 1:

   Add the following to the configured “ip dhcp pool” for a CMP IP Address of 10.234.2.206:

   ```
   option 43 hex 010c.3130.2e32.3334.2e32.2e32.3036
   ```

   Actual representation of bytes:

   ```
   01 = Type code 01
   0C = Length 12 (12 bytes make up the IP Address
    10.234.2.206)
   10.234.2.206 in hex = 31 30 2e 32 33 34 2e 32 2e 32 30
    36
   ```

   Example 2:

   Add the following to the configured “ip dhcp pool” for a CMP FQDN of cmp35.jgmb.com:

   ```
   option 43 hex 010c.3130.2e32.3334.2e32.2e32.3036
   ```

   Actual representation of bytes:

   ```
   01 = Type code 01
   0E = Length 14 (14 bytes make up the FQDN
    cmp35.jgmb.com)
   cmp35.jgmb.com in hex = 63 6d 70 33 35 2e 6a 67 6d 62 2e
    63 6f 6d
   ```
4) Pre-configuration of the DHCP server is complete.

After the DHCP server is configured additional simplified installation steps are required prior to installation of an OpenScape Session Border Controller.

2.2.5 How to Add an Endpoint in OpenScape Voice for OpenScape SBC

Proceed as follows create an endpoint in OpenScape Voice; required to create an OpenScape SBC for Simplified Installation Options 1-4:

Prerequisites

Adequate administrative permissions.

Endpoint Profiles must be configured prior to adding endpoints.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** > **OpenScape Voice** and select the **Business Group icon** within the Navigation Bar in the Common Management Platform.

2) Select the **<Business Group>** in the **Available Business Groups** pull-down associated the Branch to be viewed.

The Business Group selected appears in the Available Business Groups pull-down.

3) Select the **Members** > **Endpoints** in the Navigation Tree.

The system presents the **Endpoints** view in the Work Area with a current list of all endpoints (e.g., SBCs and branch offices) associated with the selected Business Group.

4) Proceed as follows to create a new OpenScape SBC endpoint (Central SBC):

a) Click the **Add...** button.

The **General tab** dialog is displayed by default.

b) Fill in the **Name**, select the **Registered** checkbox (indicates static Registered), select an Endpoint Profile in the **Profiles** selection list and configure **other required** fields in the general tab work area.

> **NOTICE:** The register checkbox will be grayed out until the Type to be selected is “**Static**” on the **SIP** tab.
>
> The Endpoint Profile must be configured before adding an endpoint.

c) Navigate to the **SIP tab** and configure the appropriate fields in the work area.

Because OpenScape SBC is deployed as a SIP proxy and because it does not authenticate the remote subscribers that use the SBC to register with the OSV, the endpoint must not be configured as "Trusted".

d) Navigate to the **Attributes tab** and checkmark the appropriate attributes in the work area.

Example: To create an endpoint the following parameters must be configured:

- **SIP Proxy** - Checked
- **Route via Proxy** - Checked
- **Allow Proxy Bypass** - Unchecked
- **Public/Offnet Traffic** - Checked
- **Enable Session Timer** - Checked

e) Navigate to the **Aliases tab** and configure the Alias IP address. If using OpenScape Branch with Redundancy then Alias must include redundant IP and Physical IP addresses for both OpenScape Branch nodes.

f) Continue as described in the *Managing Branch Offices* chapter in the *OpenScape Voice Assistant* documentation.

The OpenScape SBC (Central SBC) **endpoint** is now created.

The OpenScape “SBC” must now be configured in the OpenScape Voice Assistant database and further configured in the OpenScape SBC Assistant.

5) To configure the OpenScape SBC in the OpenScape Voice Assistant database, select the **Branch Office List** in the Navigation Tree.

The system presents the **Branch Office List** view in the Work Area with a current list of all SBCs and branch offices associated with the selected Business Group.

6) Proceed as follows to create a new SBC:
   a) Click the **Add...** button.

      The **<BG name> - Add Branch Office** dialog is displayed.
   b) Fill in the **Branch Office Name** and **Representative End Point** fields.
   c) Select a numbering plan for the SBC from the **Numbering Plan** selection list.
   d) Select an office code from the **Office Code** selection list.
   e) Select the routing area of the SBC in the **Routing Area** selection list.
   f) Check the **This is a Branch Office of type OpenScape Branch** checkbox in the OpenScape Branch Type field area in the **General** tab.
   g) Continue as described in the *Managing Branch Offices* chapter in the *OpenScape Voice Assistant* documentation.

The Endpoint is added to the OpenScape Voice Assistant database.

NOTICE: The OpenScape SBC must be further configured in the OpenScape SBC Assistant.

NOTICE: The OpenScape SBC Assistant Overview work area will display the endpoint for OpenScape SBC **Status** as **Inventory**

2.2.6 How to Add or Delete an OpenScape SBC to OpenScape SBC Assistant

Proceed as follows to add an OpenScape SBC to OpenScape SBC Assistant for Simplified Installation Options 1-4:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under Administration.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBC devices.

3) Proceed as follows to assign a new OpenScape SBC:

a) Click the **Add...** button.

The **Add OpenScape SBC** dialog is displayed.

b) Select the associated **Comm System** by clicking the "**...**" button and selecting a Comm system from the **Comm Systems** dialog.

c) Click the **OK** key to save the Comm System.

The **Add OpenScape SBC** dialog is re-displayed and the Comm System information is shown.

d) Select the associated **Business Group** by clicking the "**...**" button and selecting a Business Group from the **Business groups** dialog.

e) Click the **OK** key to save the Business Group.

The **Add OpenScape SBC** dialog is re-displayed and the Business Group information is shown.

f) Select the associated **Endpoint** by clicking the "**...**" button and selecting a Endpoint from the **Endpoint** dialog.

The following fields are populated:

The associated OpenScape SBC Name in the **Central SBC Name** field

The associated OpenScape SBC IP Address in the **IP Address** field

g) The **Communicating over Secured channel** checkbox indicates the status of the OpenScape SBC device. When "unsecured" (unchecked) allows the OpenScape SBC (identified by logical ID) to request an authentication statement. The checkbox is set to unchecked and grayed out by default when the OpenScape SBC is first added to the OpenScape SBC Assistant. Once the OpenScape SBC requests an authorization statement and the OpenScape SBC Assistant sends the authorization statement; the checkbox is automatically checked and the OpenScape SBC is placed in Secured Mode (the **Security status** is updated to **Secured Mode**).

> **NOTICE: Communicating over Secured channel** checkbox must be unchecked to reinstall an OpenScape SBC using simplified installation. Unchecking the checkbox will revoke the current authentication statement and allow the OpenScape SBC to request a new authentication statement.

h) Click the **OK** key to save the Endpoint.

The **Add OpenScape SBC** dialog is re-displayed and the Endpoint information is shown.

i) Click the **OK** key to save the OpenScape SBC endpoint that was created under OpenScape Voice.

The **Add OpenScape SBC** dialog is closed and the **OpenScape SBC Overview** is displayed. OpenScape SBC assigned endpoint information is shown with a **Status** = **Inventory**.

When the OpenScape SBC is added to the OpenScape SBC Assistant, from that point the OpenScape SBC Assistant will be able to administer this OpenScape SBC.

4) Proceed as follows to remove an existing SBC device from the list:
   a) Select the OpenScape SBC from the **OpenScape SBC Overview** work area by checking the associated checkmark box.
   b) Click the **Delete** button in the work area.

      The corresponding record will be deleted from the OpenScape SBC Assistant’s database.

2.2.7 How to Configure the Software Load and Hardware Type

Proceed as follows to configure the Software Load to be downloaded to the server and the Hardware Type of the server for the OpenScape SBC for Simplified Installation Options 1-4:

Prerequisites

The software load to be downloaded to the server, must be pre-loaded to the Common Management Platform (CMP) Software Repository.

The **Allowed to request a security Authentication Statement** parameter (**Configuration** > **OpenScape SBC** > **Administration** > **OpenScape SBC List > Edit an existing OpenScape SBC > Configuration Installation button**) must be enabled to allow communication between the CMP and OpenScape SBC.

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under Administration.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBC devices.
3) Select the OpenScape SBC from the **OpenScape SBC Overview** in work area by checking the associated checkbox.

   The **Edit...** button becomes active in the **OpenScape SBC Overview** Work Area.
4) Click the **Edit...** button in work area.

   The **Edit OpenScape SBC** dialog becomes active.
5) Click the **Configure Installation** button.

   The **Installation Info** dialog becomes active.
6) Select the **Software load** from the pull-down menu in the general work area e.g., V8 R0.02.0.
7) Select the **Hardware Type** from the pull-down menu in the general work area. Possible values are based on the current hardware supported e.g., X3250, X3550, RX330, RX200, ...

8) Checkmark the **Installation** checkbox if the simplified installation method is to be used to install Hardware. Setting of this flag is mandatory for simplified installation.

> **NOTICE:** The **Communicating over secured channel** checkbox in the General Tab is unchecked by default the first time. When the installation is completed, this parameter is set automatically. This parameter must be unchecked manually if the server is to be reinstalled.

9) Click the **OK** button.

The **Installation info** dialog closes and the **Edit OpenScape SBC** dialog appears.

10) Click the **OK** button.

The **Edit OpenScape SBC** dialog closes and the **OpenScape SBC Overview** window appears with the OpenScape SBC updated.

2.2.8 How to Configure the Data Configuration File

Proceed as follows to configure the data configuration file for the OpenScape SBC for Simplified Installation Options 1-4:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under Administration.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBC devices.

3) Select the OpenScape SBC from the **OpenScape SBC Overview** in work area by checking the associated checkbox.

The **Edit...** button becomes active in the **OpenScape SBC Overview** Work Area.

4) Click the **Edit...** button in work area.

The **Edit OpenScape SBC** dialog becomes active.

5) Click the **Configure Installation** button.

The **Installation Info** dialog becomes active.

6) Select the **Data Configuration File** tab.

The **Data Configuration File** dialog is displayed with the current data configuration file displayed for the OpenScape SBC.

7) Click the **Browse...** button in the work area.

The browser dialog is displayed.

8) Select the specific Data Configuration file.

Only one data file can be used by the OpenScape SBC.

NOTICE: Only XML files are allowed (no WAV files).

NOTICE: When upgrading a legacy system to V8 (or above) the XML configuration file must be inspected and modified when it gets loaded via the GUI. The Duplex Mode and MTU Size parameters (newly configurable in V8) must be added to the file and set to the default values (Duplex=Full, Speed=1000). Any manual changes that the customer made to these parameters prior to the upgrade will need to be reapplied after the upgrade using the GUI interface.

9) Click the **Add...** button in the **Data Configuration File** work area.

The **Data Configuration File** dialog is updated with the selected Data Configuration file.

10) Click the **OK** button.

The **Installation info** dialog closes and the **Edit OpenScape SBC** dialog appears.

11) Click the **OK** button.

The **Edit OpenScape SBC** dialog closes and the **OpenScape SBC Overview** window appears with the OpenScape SBC now updated.

2.2.9 How to Configure the MAC Address

Proceed as follows to configure the MAC address to an OpenScape SBC for Simplified Installation Option 1 only:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under Administration.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBC devices.

3) Select the OpenScape SBC from the **OpenScape SBC Overview** in work area by checking the associated checkbox.

The **Edit...** button becomes active in the **OpenScape SBC Overview** Work Area.

4) Click the **Edit...** button in work area.

The **Edit OpenScape SBC** dialog becomes active.

5) Click the **Configure Installation** button.

The **Installation info** dialog becomes active.

6) Select the **Software load** from the pull-down menu in the general work area (if not already configured).

7) Select the **Hardware Type** from the pull-down menu in the general work area (if not already configured).

8) Enter the LAN MAC address in the **MAC address** field in the general work area is used for simplified installation and licensing. The LAN MAC address must be entered in the form of e.g., 5C:F3:FD:31:DK:52 (not case sensitive).

9) The LAN MAC address in the **MAC Address Node 2** field in the general work area is automatically populated. This address is used for redundant systems and licensing.

10) Click the **OK** button.

The **Installation info** dialog closes and the **Edit OpenScape SBC** dialog appears.

11) Click the **OK** button.

The **Edit OpenScape SBC** dialog closes and the **OpenScape SBC Overview** window appears with the OpenScape SBC now updated.

2.2.10 How to Install Hardware for Simplified Installation

Proceed as follows to install an OpenScape SBC Hardware using Simplified Installation:

Prerequisites

The OpenScape hardware is pre-loaded with all required installation software based on the installation option.

The Common Management Platform (CMP) and OpenScape SBC Assistant is pre-loaded with all required installation software and Configuration file.

The USB stick is pre-loaded with all required installation software (Options 2-4).

The URL associated with the Common Management Platform (CMP) is pre-configured into the DHCP server (Option 1-2).

The DHCP server is configured and operational (Options 1-3).

The MAC address (LAN MAC) in configured in the OpenScape SBC Assistant (Option 1 only).

The OpenScape SBC is configured in OpenScape Voice.

The simplified **Installation** parameter (checkbox) is checkmarked in the **Configure Installation> Installation Info** dialog.

The **Communicating over secured channel** checkbox in the **Edit OpenScape SBC > General Tab** is unchecked.

The OpenScape SBC is configured in OpenScape SBC Assistant with a Unique ID (MAC Address (LAN MAC) for Option 1, Logical ID is generated (not configured) for options 2-4), Software load, Hardware type.

OpenScape SBC Access to CMP (unsecured port 4709) must be configured in the OpenScape SBC Assistant prior to powering up the server. This is required to allow authentication, configuration and licensing information.

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Connect the OpenScape Server to the customer's network.
2) Plug the USB stick into the OpenScape server. Required for Options 2-4).
3) Power up the OpenScape Server.

   The following installation functions take place:

   - OpenScape SBC will send a DHCP Request (Options 1-3)
   - Once DHCP data is received it will reboot to apply temporary IP address and connect to the network.
   - Once the temporary IP address is set, the OpenScape SBC will contact the CMP server.
   - The SBC device is validated by the OpenScape SBC Assistant. For Option 1 the MAC address (LAN MAC) is used for validation and for Options 2-4, the logical ID is used for validation.
   - The SBC sends a request for a list of installation files to the OpenScape SBC Assistant.
   - The OpenScape SBC Assistant validates the request and returns a list of file names, paths and information about the http server (e.g., CMP) from which to retrieve the files. The file list can include file information related to sw load version, configuration file name that need to be downloaded by the OpenScape SBC device. OpenScape SBC Assistant also updates the device state in the GUI.
   - The OpenScape SBC device Server installs the files using HTTP(s) based on information in the file provided by OpenScape SBC Assistant.
   - A final boot is required to apply the xml file data and activate the software (SW) version download from the CMP.
   - The OpenScape SBC device logs the error cases and will also send alarms if possible.

4) Monitor installation progress using the OpenScape SBC Assistant. Select the **Configuration tab** > **OpenScape SBC** > **OpenScape SBC list** in the navigation tree. Refresh the OpenScape SBC Overview work area display.
   a) Click the **Refresh All** button to update the OpenScape SBC Overview status information.
   b) Or, Select the device of interest in the work area and click the **Refresh Selected** button to update the OpenScape SBC Overview status information.

   The following values are displayed in the Status column of the OpenScape SBC Overview work area:

   - **Inventory** - Indicates the OpenScape SBC system is configured in the Assistant but not installed.
   - **Authenticated** – Indicates the OpenScape SBC platform has contacted the OpenScape SBC Assistant with all appropriate credentials.
   - **Installation started** – Indicates that the OpenScape SBC has all the data necessary and started the installation process.
   - **File Transfer Started** - Indicates that the File Transfer has been started by the OpenScape SBC.
   - **File Transfer Successful**.
   - **File Transfer failed**: <filename>-<HttpErrorCode> - Indicates that one of the file has failed to transfer.
   - **Booting** - Indicates the Boot of the OpenScape SBC has started.
   - **Boot Failed** (and reason if provided) - Indicates that the OpenScape SBC failed to come up after the boot. No communication is possible.
   - **Normal/Survival** - The appliance has successfully been installed and ready for the call handling.
   - **Unreachable** – check alarms.

5) Troubleshoot and correct any errors or alarms during installation and reinstall.
6) The OpenScape SBC device alerts when the installation is complete. If the Installation is successful the OpenScape SBC device will beep once, pause, and repeat. Beeps will occur for 10 cycles.

After the process is concluded the OpenScape SBC device is installed and operational.

2.2.11 How to Troubleshoot Installation Errors and Alarms

The OpenScape SBC and SBC Assistant provide error log information locally. This information must be retrieved manually. The OpenScape SBC device will provide audible beeps, if hardware supports, to the installer so the installer can determine the nature of the problem. If the OpenScape SBC device knows the CMP URL it will also try to send alarms. Proceed as follows to troubleshoot audible alarm sequences that occur during Simplified Installation:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Troubleshoot and correct any alarms during installation and reinstall.

> **NOTICE:** If an error condition occurs, the OpenScape SBC will abort installation and fallback to the default IP 192.168.0.1 (park state). After the issues are resolved, the OpenScape SBC can be restarted and the simplified installation process will be restarted.

2) Beeps, pause and repeat for 10 cycles represent the following alarms:

- Cannot contact DHCP
- DHCP server did not return temporary dynamic IP for the OpenScape SBC device
- DHCP server not configured to return CMP URL

3) Beeps, pause and repeat for 10 cycles represent the following alarms:

- MAC not pre-configured in CMP
- Logical ID not pre-configured in CMP
- Lack of NW connectivity
- Cannot contact CMP

> **NOTICE:** Logical ID consists of: <OpenScape Voice Name>:<Business Group Name>:<SBC Name>

4) Beeps, pause and repeat for 10 cycles represent the following alarms:

- Installation Info unavailable
- File Transfer unsuccessful
- Boot Failure
- SOAP Responses received with negative acks
- No Response to SOAP Requests sent by the OpenScape SBC device
- SOAP Requests received that have invalid data

5) Troubleshoot and correct any errors indicated on the OpenScape SBC Assistant during installation and reinstall. Select the **Configuration** > **OpenScape SBC** > **OpenScape SBC list** in the navigation tree. Refresh the OpenScape SBC Overview work area display.

a) Click the **Refresh All** button to update the OpenScape SBC Overview work area information.

b) Or, Select the device of interest in the work area and click the **Refresh Selected** button to update the OpenScape SBC Overview work area information.

The following values are displayed in the Status column of the OpenScape SBC Overview work area:

- **Inventory** - Indicates the OpenScape SBC system is configured in the Assistant but not installed.
- **Authenticated** – Indicates the OpenScape SBC platform has contacted the OpenScape SBC Assistant with all appropriate credentials.
- **Installation started** – Indicates that the OpenScape SBC has all the data necessary and started the installation process.
- **File Transfer Started** - Indicates that the File Transfer has been started by the OpenScape SBC.
- **File Transfer Successful**.
- **File Transfer failed**: <filename>-<HttpErrorCode> - Indicates that one of the file has failed to transfer (error log file only).
- **Booting** - Indicates the Boot of the OpenScape SBC has started.
- **Boot Failed** - Indicates that the OpenScape SBC failed to come up after the boot. No communication is possible.
- **Normal/Survival** - The appliance has successfully been installed and ready for the call handling.
- **Unreachable** – check alarms.

Information related to file transfer failure is displayed in the error log file including the name of the file that failed and the HTTP reasons for the file transfer failure returned by SBC which can include:

- 400 Bad Request
- 401 Unauthorized
- 403 Forbidden
- 404 Not Found
- 405 Method Not Allowed
- 406 Not Acceptable
- 408 Request Timeout
- 409 Conflict
- 410 Gone
- 413 Request Entity Too Large
- 414 Request-URI Too Long
- 415 Unsupported Media Type
- 422 Unprocessable Entity
- 423 Locked
- 426 Upgrade Required
- 444 No Response
- 499 Client Closed Request
- 500 Internal Server Error
- 501 Not Implemented
- 503 Service Unavailable

Error Log File Locations:

- Common Management Platform (CMP) log file name is **symphonia.log** under the following directories

  - Offboard: **/var/siemens/common/log/**

  - Onboard: **/log/**
- OpenScape SBC log file name is **autoinstall.log** under the following directory **/opt/siemens/openbranch/var/log/openbranch/**

6) Power up the OpenScape SBC server once the errors have been corrected.

The **Communicating over Secured channel** checkbox for the OpenScape SBC configuration in the OpenScape SBC Assistant must be unchecked (Unsecured mode) to allow installation and reinstall an OpenScape SBC.

7) The OpenScape SBC device alerts when the installation is complete. If the Installation is successful the OpenScape SBC device will beep once, pause, and repeat. Beeps will occur for 10 cycles.

After the process is concluded the OpenScape SBC device is installed and operational.

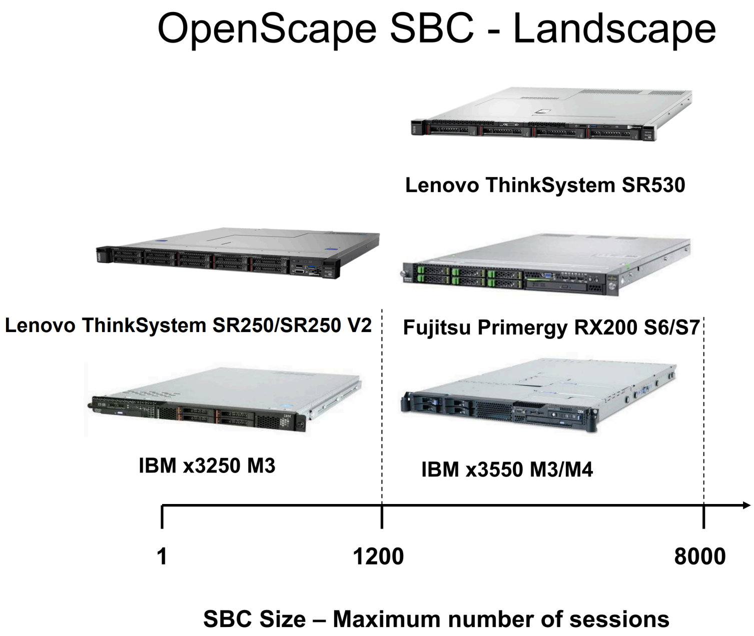
3 OpenScape Session Border Controller Hardware – Overview

The OpenScape Session Border Controller (SBC) can operate on different hardware platforms depending on the number of SBC session required.

> **NOTICE:** Only the HW servers as configured by the standard ordering positions are supported by the product house for OpenScape SBC. Deviations from the standard HW configuration are not supported.
>
> OpenScape SBC's Simplified Installation feature is supported only for server platforms that are purchased using Unify's global ordering tool and staged by Unify. The standard (manual) installation process must be used for server platforms ordered from regional suppliers.

OpenScape Session Border Controller Hardware Platforms

OpenScape SBC can be installed as virtualized on a customer's VMware environment or be installed and operated on one of the following three native hardware server platforms.

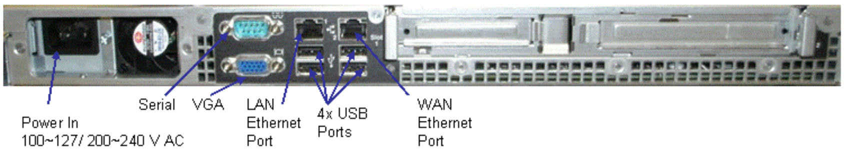

OpenScape SBC - Landscape
Lenovo ThinkSystem SR530
Lenovo ThinkSystem SR250/SR250 V2
Fujitsu Primergy RX200 S6/S7
IBM x3250 M3
IBM x3550 M3/M4
1
1200
8000
SBC Size – Maximum number of sessions

- **OpenScape Session Border Controller** that uses the IBM x3250 M3/M5/M6 or Lenovo ThinkSystem SR250/SR250 V2 supports up to 1200 SBC sessions.
- **OpenScape Session Border Controller** that uses the IBM x3550 M3/M4, Fujitsu RX200 S6/S7 or Lenovo ThinkSystem SR530 or Lenovo ThinkSystem SR630 V2 supports up to 8000 SBC sessions.

3.1 OpenScape Session Border Controller IBM/Lenovo x3250, Lenovo SR250/SR250 V2 Hardware

OpenScape Session Border Controller based on the IBM x3250 M3/M5/M6 or Lenovo SR250/SR250 V2 server supports up to 1200 SBC sessions.

OpenScape Session Border Controller IBM x3250 M3/M5/M6



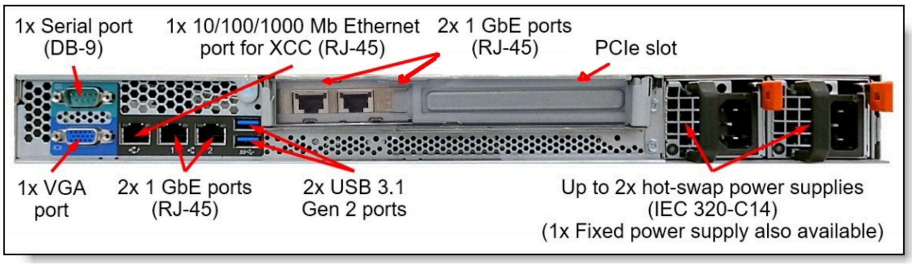
Specification:

- IBM x3250 M3/M5/M6 server
- Physical Dimension (W x H x D): 440 x 43 x 559 mm (17.3” x 1.69” x 22.0”)
- Weight: up to 12.7 Kg (28.0 lb)
- Rated Power: 100~127 / 200~240 V AC, 50-60 Hz, 351W (single power supply)
- Average Power Consumption: 75W
- Rated Heat Emission: 1263.7 kJ/h (1197.7 BTU)
- Operating Temperature: 0-35C (32-95F)

Part Numbers:

- Unify Part number: ADA601 / L30220-D600-A601

OpenScape Session Border Controller Lenovo ThinkSystem SR250/SR250 V2


1x Serial port (DB-9)
1x 10/100/1000 Mb Ethernet port for XCC (RJ-45)
2x 1 GbE ports (RJ-45)
PCIe slot
1x VGA port
2x 1 GbE ports (RJ-45)
2x USB 3.1 Gen 2 ports
Up to 2x hot-swap power supplies (IEC 320-C14) (1x Fixed power supply also available)

Specification Lenovo ThinkSystem SR250:

- Lenovo ThinkSystem SR250 server
- Physical Dimension (W x H x D): 434 x 43 x 498 mm (17.1” x 1.7” x 19.6”)
- Weight: up to 12.3 Kg (27.1 lb)
- Rated Power: 100~127 / 200~240 V AC, 50-60 Hz, 334W (single power supply)
- System Heat Output: 1139 BTU/hour
- Operating Temperature: 5-40C (41-104F)

Part Numbers:

- Unify Part number: S30122-X8000-X129

Specification Lenovo ThinkSystem SR250 V2:

- Lenovo ThinkSystem SR250 V2 server
- Physical Dimension (W x H x D): 435 x 43 x 545 mm (17.1” x 1.7” x 21.5”)
- Weight: up to 12.3 Kg (27.1 lb)
- Rated Power: 100~127 / 200~240 V AC, 50-60 Hz
- System Heat Output: 802.5 BTU/hour
- Operating Temperature: 5-40C (41-104F)

Part Numbers:

- Unify Part number: S30122-X8000-X134

RAID (Redundant array of independent disks) informationfor IBM3550, RX200 and SR530

Please refer to chapter 3 to the following document for instructions: OpenScape Voice V10, Service Manual: Installation and Upgrades, Installation Guide.

NOTICE: Only RAID1 is supported.

3.1.1 How to Install the IBM x3250 M3/M5/M6 Server Hardware

Proceed as follows to connect the cables of the IBM x3250 M3/M5/M6 server hardware for the OpenScape Session Border Controller:

Prerequisites

The safety instructions have been read and well-understood.

Step by Step

1) Refer to the IBM x3250 M3/M5/M6 rack installation instructions to install the server into the rack.

2) Attach the keyboard, mouse, and monitor cables to the server.

> **NOTICE:** If the equipment for OpenScape Voiceincludes a KVM, connect cables from the keyboard, mouse, and monitor connectors on the server to the KVM and connect the keyboard, mouse and monitor cables to the appropriate connectors on the KVM. If necessary, refer to the KVM documentation for assistance.

3) Attach the Ethernet cables.

a) Attach an Ethernet cable to the LAN switch for the local LAN and to the Ethernet interface port on the IBM x3250 server that corresponds to the LAN interface (Ethernet 1) you configured in the node.cfg. This is the core side of the OpenScape SBC that interfaces the OpenScape Voice (OSV) system.

b) For an OpenScape Session Border Controller: Attach an Ethernet cable to the LAN switch or router for the external WAN and to the Ethernet interface port on the IBM x3250 server that corresponds to the WAN interface (Ethernet 2) you configured in the node.cfg. This is the access side of the OpenScape SBC that interfaces the SIP Trunk Service Provider, remote users, or remote OpenScape Branches.

4) Attach the power cord to the server and to the power receptacle.

5) Turn on the server.

> **NOTICE:** The IBM x3250 server requires the server boot sequence in the BIOS to be updated. The following steps are required to update the server boot sequence and date and time settings.

6) At boot up, wait and press **F1** to enter the BIOS setup when the option “<F1> Setup” is available.

The System Configuration and Boot Management window is displayed.

7) Use the **arrow key** to navigate to the **Boot Manager** and press **Enter**.

The Boot Management window is displayed.

8) Select **Add Boot Option** and press **Enter**.

9) Select **USB Storage** and press **Enter**.

10) Press **Esc** to exit and go back to the Boot Manager window.

The System Configuration and Boot Management window is displayed.

11) Select **Change Boot Order** and press **Enter**.

12) Press **Enter** again to change the order.

13) Using the “+” and “-” keys ensure the order is as follows: USB Storage, CD/DVD Rom, Hard Disk 0 and then press **Enter**.

The settings are temporarily saved.

14) Select **Commit Changes** to save changes.

15) Press **Esc** to progress to the **Main Screen**.

> **NOTICE:** The banner at the bottom of the Main screen describes how to select and change the values in the time and date fields on the Main screen. It also describes how to select screens.

The Main screen of the BIOS Setup Utility is displayed.

16) From the main menu of the **Configuration/Setup Utility**, select Date and Time and press **Enter**.

17) In the **Date and Time** screen, ensure that the date and time is correct, and then press the **Esc** key to return to the main menu of the Configuration/ Setup Utility.

18) From the main menu of the Configuration/Setup Utility, select **Exit Setup** and press **Enter**.

The **Exit Setup** screen is displayed.

19) In the **Exit Setup** screen, select **Yes, save and exit the Setup Utility,** and press **Enter** to confirm that you want to exit.

The system will reset.

3.1.2 How to Install the Lenovo SR250/SR250 V2 Server Hardware

Proceed as follows to connect the cables of the Lenovo SR250/SR250 V2 server hardware for the OpenScape Session Border Controller.

Prerequisites

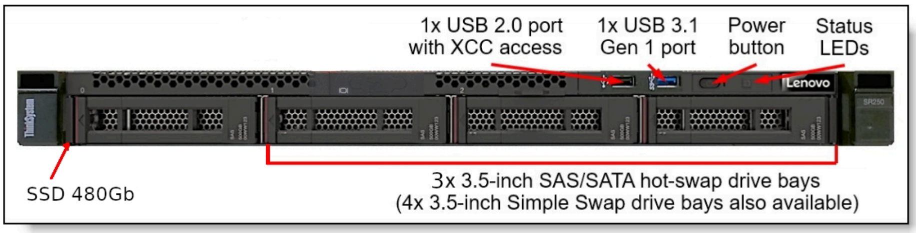
This section describes the equipment needed on the Lenovo SR250/SR250 V2. All necessary hardware comes pre-installed. You can find the steps necessary to assemble the hardware, connect the cables and load the necessary firmware.

> **IMPORTANT:** Lenovo SR250 V2 is available starting from V10R3.3.0.

Step by Step

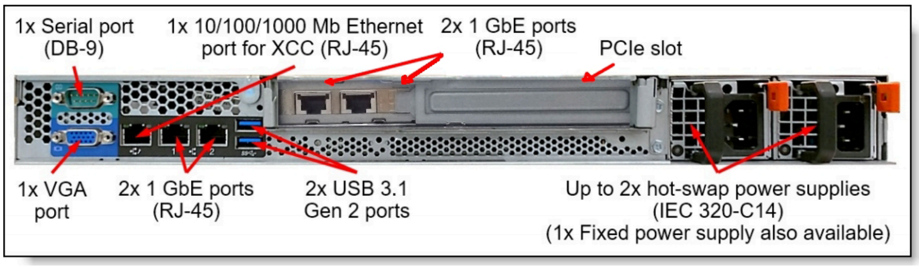
1) Refer to the Lenovo SR250/SR250 V2 rack installation instructions to install the server into the rack.

2) Install the disk drive. The image below shows the location of the drive. The system comes with a total of 4 3.5-inch drive bays.

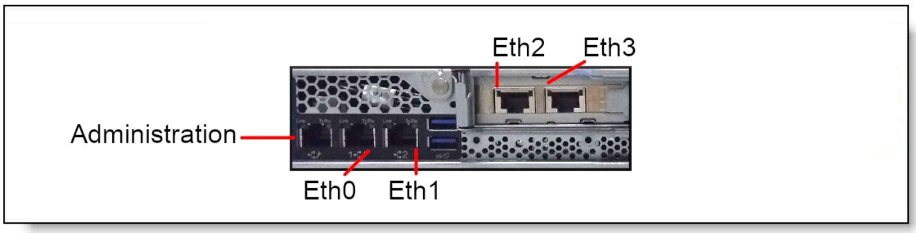

1x USB 2.0 port with XCC access
1x USB 3.1 Gen 1 port
Power button
Status LEDs
SSD 480Gb
3x 3.5-inch SAS/SATA hot-swap drive bays
(4x 3.5-inch Simple Swap drive bays also available)

To remove a drive, slide the release latch to the right with one finger while using another finger to grasp the black drive handle and pull the hard disk drive out of the drive bay.

3) Connection Panel in the rear of the Lenovo SR250/SR250 V2 server. The system comes pre- installed with five onboard ports (two Integrated 1 GbE and one 10/100/1000 MbE for XCC on Motherboard), and a Broadcom Limited 2 port NX BCM5720 GbE. The image below gives a general overview of the connection panel in the rear of the Lenovo SR250/SR250 V2 server.


1x Serial port (DB-9)
1x 10/100/1000 Mb Ethernet port for XCC (RJ-45)
2x 1 GbE ports (RJ-45)
PCIe slot
1x VGA port
2x 1 GbE ports (RJ-45)
2x USB 3.1 Gen 2 ports
Up to 2x hot-swap power supplies (IEC 320-C14)
(1x Fixed power supply also available)

4) Network port assignment. The following diagrams show the Ethernet port assignments for the Lenovo SR250/SR250 V2.



5) Power on the server

6) At boot up, press F1 to enter the UEFI setup when the option **<F1> System Setup** is available.

Press many times until the option symbol turns blue.

7) After the **System Summary** screen appears, go to **UEFI Setup** > **System Settings** > **Legacy BIOS** and enable the option **Legacy BIOS**

8) Go to **Boot Manager** > **Boot Modes** and select **Legacy Modes**

9) Save the configuration by clicking **Save** in the right corner

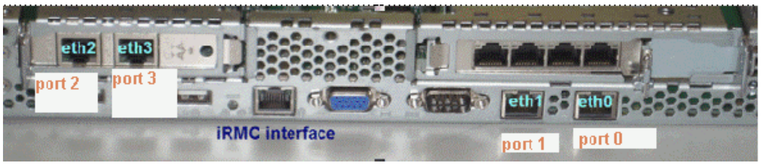
10) Back to **Boot Manager**, select **Reboot System**

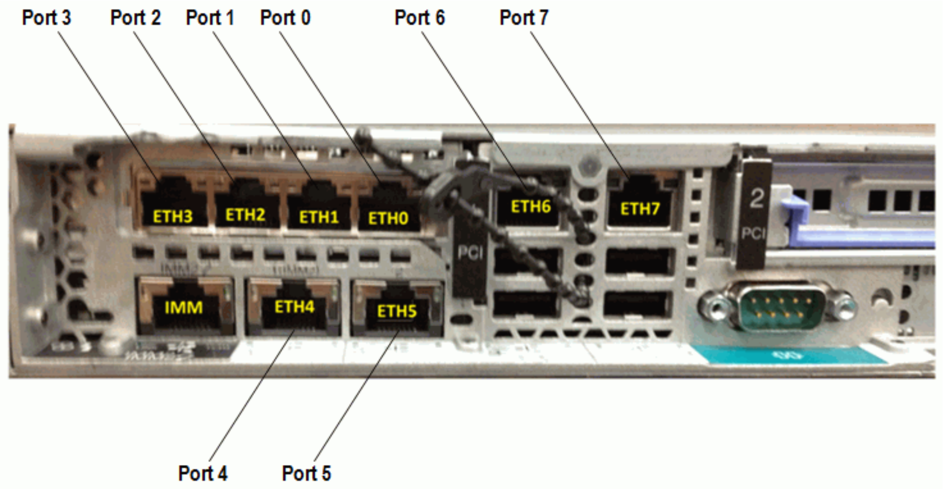
3.1.3 OpenScape Session Border Controller IBM x3550 M3/M4 or Fujitsu Primergy RX200 S6/S7 Hardware

OpenScape Session Border Controller based on the IBM x3550 (M3/M4) or Fujitsu Primergy RX200 S6/S7 hardware can support up to 4000 SBC sessions.

OpenScape Session Border Controller - IBM x3550 M4

OpenScape Session Border Controller - IBM x3550 M3

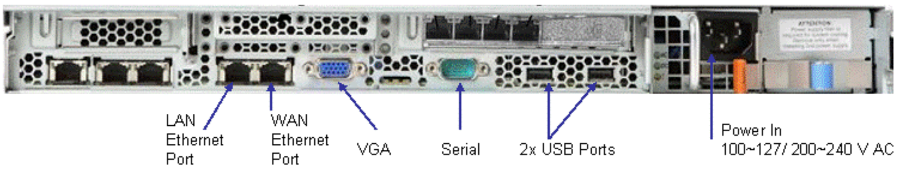




The IBM x3550 M4 is a new server in the IBM family of x3550 servers. Since the IBM x3550 servers are almost alike with only a few differences when it comes to installation, most of the references in this document will indicate IBM x3550 M2/M3/M4 meaning the section or description applies to the IBM x3550 M2, IBM x3550 M3 and IBM x3550 M4 servers. If differences apply, then they will be indicated as to which server they apply to.

Housed within a rack-mountable enclosure, the IBM x3550 M4 server is equipped for OpenScape Session Border Controller as follows:

- Processor: Two 2.00 GHz 6-Core Intel Xeon E5-2620 CPUs
- Memory: 32 GB of Double Data Rate 3 (DDR3) memory
- Hard disk drive: Two 300 GB hot-swappable HDDs in RAID1
- CD/DVD drive
- Disk controller: Internal on-board RAID controller
- Ethernet interfaces
- Universal Serial Bus (USB) ports: Six (two at the front, four at the back)
- Remote Supervision: One Intel Management Module with optional Virtual Key Media (VMK)
- Power supply: Two hot-swappable AC power supplies, DC power is optional



Specification:

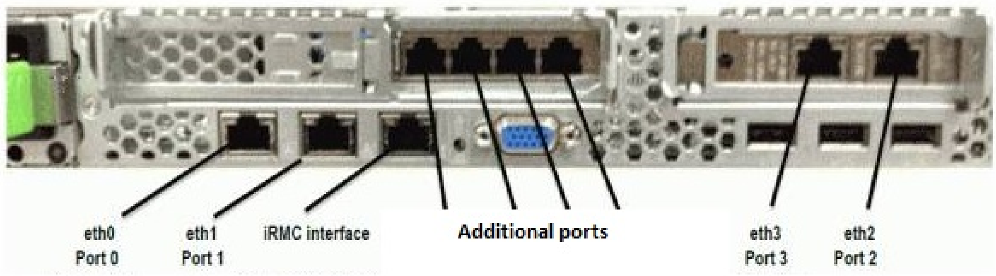
- IBM x3550 M3
- Physical Dimension (W x H x D): 440 x 44 x 711 mm (17.3” x 1.7” x 28.0”)
- Weight: up to 15.4 Kg (34.0 lb)
- Rated Power: 100~127 / 200~240 V AC, 50-60 Hz, 351W
- Average Power Consumption: 180W
- Rated Heat Emission: 1263.6 kJ/h (1197.7 BTU)
- Operating Temperature: 10-35C (50-95F)

Part Numbers:

- ADA569 / L30220-D600-A569
- BZF101 / L30280-Z600-F101 (Power Cord, USA Variant)
- BZF102 / L30280-Z600-F102 (Power Cord, UK Variant)
- BZF105 / L30280-Z600-F105 (Power Cord with Straight Appliance Connector, EURO Variant)
- BZF107 / L30280-Z600-F107 (Power Cord, BRA Variant)
- BZF108 / L30280-Z600-F108 (Power Cord, ARG Variant)

NOTICE: The IBM x3550 M2 is no longer available for new orders and will support OpenScape Branch V1R4 and V2.

OpenScape Session Border Controller - Fujitsu Primergy RX200 S7

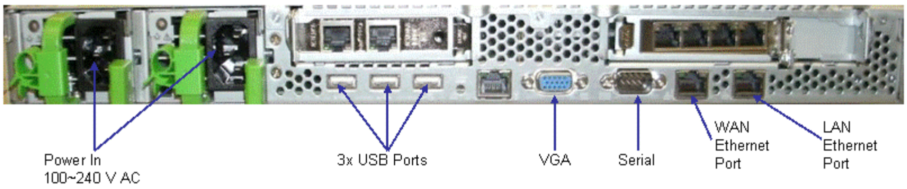


The FTS RX200 S7 is a new server in the FTS family of RX200 servers. Since the FTS RX200 servers are almost alike with only a few differences when it comes to installation, most of the references in this document will indicate FTS RX200 S6/S7 meaning the section or description applies to the FTS RX200 S6 and the FTS RX200 S7 servers. If differences apply, then they will be indicated as to which server they apply to.

Housed within a rack-mountable enclosure, the FTS RX200 S7 server is equipped for OpenScape Session Border Controller as follows:

- Processor: Two 2.00 GHz 6-Core Intel Xeon E5-2620 CPUs
- Memory: 32 GB of Double Data Rate 3 (DDR3) memory
- Hard disk drive: Two 300 GB hot-swappable HDDs in RAID1
- CD/DVD drive
- Disk controller: Internal on-board RAID controller
- Ethernet interfaces
- Universal Serial Bus (USB) ports: Five (two at the front, three at the back)
- Remote Supervision: One integrated Remote Management Controller (iRMC)
- Power supply: Two hot-swappable 110/220 AC power supplies

OpenScape Session Border Controller - Fujistu Primergy RX200 S6



Specification:

- Fujitsu Primergy RX200 S6
- Physical Dimension (W x H x D): 431 x 43 x 762mm (18” x 1.69” x 30.0”)

- Weight: up to 17 Kg (37.5 lb)
- Rated Power: 100~240 V AC, 50-60 Hz, 549W (redundant power supplies)
- Average Power Consumption: 193W
- Rated Heat Emission: 1976.4 kJ/h (1873.3 BTU)
- Operating Temperature: 10-35C (50-95F)

Part Numbers:

- Unify Part number: ADA603 / L30220-D600-A603

3.1.4 How to Install the IBM x3550 M3/M4 Server Hardware

Proceed as follows to connect the cables of the IBM x3550 M3/M4 server hardware for the OpenScape Session Border Controller:

Prerequisites

The safety instructions have been read and well-understood.

Step by Step

1) Refer to the IBM x3550 M3/M4 rack installation instructions to install the server into the rack.

2) Attach the keyboard, mouse (the IBM x3550 M3/M4 requires a USB keyboard and mouse: a PS/2 to USB adaptor can be used in most cases), and monitor cables to the server.

> **NOTICE:** If the equipment for IBM x3550 M2includes a KVM, connect cables from the keyboard, mouse, and monitor connectors on the server to the KVM and connect the keyboard, mouse and monitor cables to the appropriate connectors on the KVM. If necessary, refer to the KVM documentation for assistance.

3) Attach the Ethernet cables.

a) Attach an Ethernet cable to the LAN switch for the local LAN and to the Ethernet interface port on the IBM x3550 server that corresponds to the LAN interface you configured in the node.cfg. This is the core side of the OpenScape SBC that interfaces the OpenScape Voice (OSV) system.

b) For an OpenScape Session Border Controller: Attach an Ethernet cable to the LAN switch or router for the external WAN and to the Ethernet interface port on the IBM x3550 server that corresponds to the WAN interface you configured in the node.cfg. This is the access side of the OpenScape SBC that interfaces the SIP Trunk Service Provider, remote users, or remote OpenScape Branches.

4) Attach the power cord to the server and to the power receptacle.

5) Turn on the server.

> **NOTICE:** The IBM x3550 server requires the server boot sequence in the BIOS to be updated. The following steps

are required to update the server boot sequence and date and time settings.

6) At boot up, wait and press **F1** to enter the BIOS setup when the option “<F1> Setup” is available.

The System Configuration and Boot Management window is displayed.

7) Use the **arrow key** to navigate to the **Boot Manager** and press **Enter**.

The Boot Management window is displayed.

8) Select **Add Boot Option** and press **Enter**.

9) Select **USB Storage** and press **Enter**.

10) Press **Esc** to exit and go back to the Boot Manager window.

The System Configuration and Boot Management window is displayed.

11) Select **Change Boot Order** and press **Enter**.

12) Press **Enter** again to change the order.

13) Using the “+” and “-” keys ensure the order is as follows: USB Storage, CD/DVD Rom, Hard Disk 0 and then press **Enter**.

The settings are temporarily saved.

14) Select **Commit Changes** to save changes.

15) Press **Esc** to progress to the **Main Screen**.

NOTICE: The banner at the bottom of the Main screen describes how to select and change the values in the time and date fields on the Main screen. It also describes how to select screens.

The Main screen of the BIOS Setup Utility is displayed.

16) From the main menu of the **Configuration/Setup Utility**, select Date and Time and press **Enter**.

17) In the **Date and Time** screen, ensure that the date and time is correct, and then press the **Esc** key to return to the main menu of the Configuration/Setup Utility.

18) From the main menu of the Configuration/Setup Utility, select **Exit Setup** and press **Enter**.

The **Exit Setup** screen is displayed.

19) In the **Exit Setup** screen, select **Yes, save and exit the Setup Utility,** and press **Enter** to confirm that you want to exit.

The system will reset.

3.1.5 How to Install the Fujitsu RX200 S6/S7 Server Hardware

Proceed as follows to connect the cables and set up the Fujitsu RX200 S6/S7 server hardware for the OpenScape Session Border Controller:

Prerequisites

The safety instructions have been read and well-understood.

Step by Step

1) Refer to the FSC RX200 rack installation instructions to install the server into the rack.

2) Attach the keyboard, mouse, and monitor cables to the server.

> **NOTICE:** If the equipment for OpenScape Voiceincludes a KVM, connect cables from the keyboard, mouse, and monitor connectors on the server to the KVM and connect the keyboard, mouse and monitor cables to the appropriate connectors on the KVM. If necessary, refer to the KVM documentation for assistance.

3) Attach the Ethernet cables.

a) Attach an Ethernet cable to the LAN switch for the local LAN and to the Ethernet interface port on the Fujitsu RX200 server that corresponds to the LAN interface you configured in the node.cfg. This is the core side of the OpenScape SBC that interfaces the OpenScape Voice (OSV) system.

b) For an OpenScape Session Border Controller: Attach an Ethernet cable to the LAN switch or router for the external WAN and to the Ethernet interface port on the Fujitsu RX200 server that corresponds to the WAN interface you configured in the node.cfg. This is the access side of the OpenScape SBC that interfaces the SIP Trunk Service Provider, remote users, or remote OpenScape Branches.

> **NOTICE:** Ensure that the Ethernet switch or switches are configured for VLAN operation. Refer to the Ethernet switch manufacturer’s documentation for instructions.

4) Attach the power cord to the server and to the power receptacle.

5) Turn on the server

> **NOTICE:** The Fujitsu server requires LSI RAID creation. The following steps will setup the internal LSI controller and disks into a mirrored pair. The LSI RAID Creation functionality is in the Setup Application.

Shortly after power is applied the following prompt should appear on the **System Console** screen: **Press <Ctrl><H> for WebBIOS or press <Ctrl><Y> for Preboot CLI**.

6) Press **<Ctrl><H>** to get to the WebBIOS screen.

The **Adapter Selection** screen is displayed.

7) Click the **Start** button to advance to the WebBIOS Main screen.

The **WebBIOS** main screen is displayed with the physical view as the default.

8) Select the **Configuration Wizard**.

The **MegaRAID BIOS Config Utility Configuration Wizard** screen is displayed.

9) Select **New Configuration** and click the **Next** button.

The **MegaRAID BIOS Config Utility Confirm Page** is displayed.

10) Click the **Yes button since this is a new system. This will clear the current configuration**.

    The **MegaRAID BIOS Config Utility Configuration Wizard** screen is displayed.

11) Select **Automatic Configuration** and select **Redundancy when possible** in the pull down; then click the **Next** button.

    The **MegaRAID BIOS Config Utility Wizard - Preview** screen is displayed. This screen provides a preview of the new virtual RAID to be created.

12) Click the **Accept button**.

    The **MegaRAID BIOS Config Utility Confirm Page** is displayed and a confirmation prompt to create the new virtual RAID appears.

13) Click the **Yes button to save the configuration.**

    The **MegaRAID BIOS Config Utility Confirm Page** is displayed and a prompt to initialize the Virtual Drives appears.

14) Click the **Yes button to start the initialize virtual drives sequence.**

    The **MegaRAID BIOS Config Utility Virtual Drives** screen is displayed.

15) Select **Fast Initialize** and click the **Go** button.

    The **MegaRAID BIOS Config Utility Confirm Page** is displayed and a confirmation prompt to initialize the virtual drives appears.

16) Click the **Yes** the button to proceed to initialize the virtual drives and click the **Home** button to return to the main page.

    The **MegaRAID BIOS Config Utility Virtual Configuration** screen is displayed and should now indicate the presence of a Virtual RAID.

17) Select the **Boot tab**

    The **System Console Boot** screen is displayed.

18) Using the up and down keys select the USB Key (storage) and other storage devices, one at a time.

19) Using the “+” and “-” keys ensure the order is as follows: USB Storage, CD/DVD Rom, Hard Disk 0.

    Verify there is no CD/DVD in the drive prior to configuring the boot sequence to guarantee booting from the USB.

20) Save the configuration

21) Select **Exit**

    The **Exit Confirmation** screen is displayed.

22) Click the **Yes button to exit.**

    The configuration is updated.

3.1.6 How to Install the Lenovo SR530 Server Hardware

Proceed as follows to connect the cables of the Lenovo SR530 server hardware for the OpenScape SBC 20000 model:

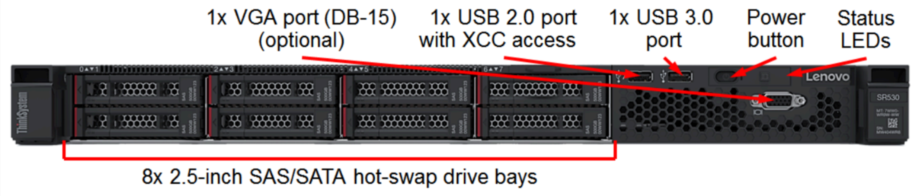
Prerequisites

This section describes the equipment needed on the Lenovo SR530. All necessary hardware comes pre-installed. You can find the steps necessary to assemble the hardware, connect the cables and load the necessary firmware.

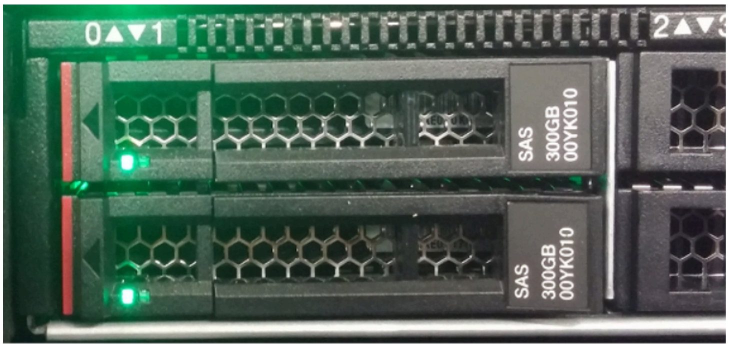
Step by Step

1) Refer to the Lenovo SR530 rack installation instructions to install the server into the rack.

2) Install the disk drive.The image below shows the location of the two drives. The system comes with a total of 8 2.5-inch drive bays.

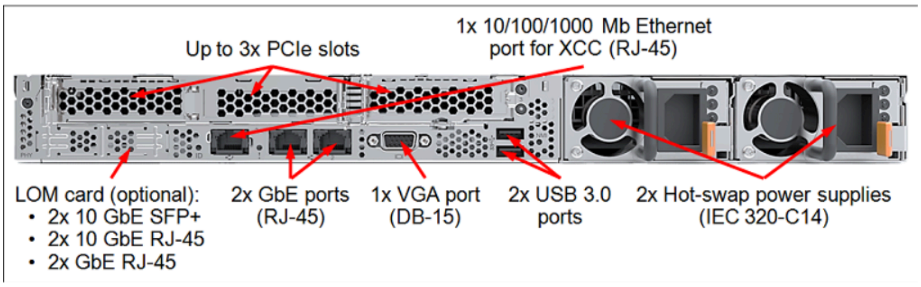

1x VGA port (DB-15) (optional)
1x USB 2.0 port with XCC access
1x USB 3.0 port
Power button
Status LEDs
8x 2.5-inch SAS/SATA hot-swap drive bays

The image below is a close-up of the drives, with the two leftmost bays populated with hard disks.



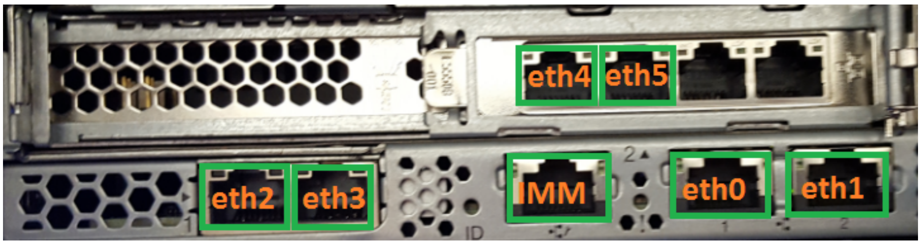
To remove a drive, slide the blue release latch to the right with one finger while using another finger to grasp the black drive handle and pull the hard disk drive out of the drive bay.

3) Connection Panel in the rear of the Lenovo SR530 server.The image below gives a general overview of the connection panel in the rear of the Lenovo SR530 server.



4) Installing the PCI.PCI installation is not required. The system comes pre-installed with four onboard ports (two Integrated one GbE and 2x1/10/100 GbE LOM - LAN on Motherboard), and an Intel 4 port PCI Express card. These are identified in the table below:

NOTICE: The four onboard ports provide only gigabit support.



5) Network port assignment. The following diagrams show the Ethernet port assignments for the Lenovo SR530, for a duplex and a simplex setup.

After adding and wiring all hardware to the machine, continue with the UEFI configuration, RAID creation and firmware updates. If you are using KVM devices connect it to the server prior to initial boot.

3.1.7 How to Install the Lenovo SR630 V2 Server Hardware

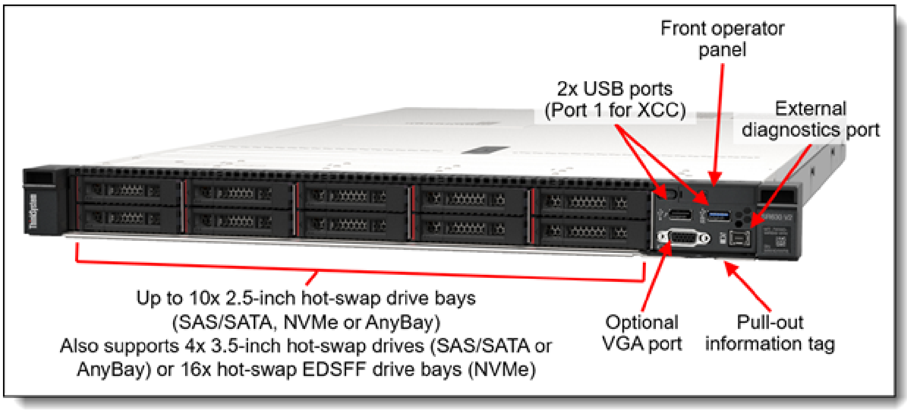
This section describes the equipment needed on the Lenovo SR630 V2. All necessary hardware comes pre-installed. You can find the steps necessary to assemble the hardware, connect the cables and load the necessary firmware.

Proceed as follows to connect the cables of the Lenovo SR630 V2 server hardware for the OpenScape SBC 20000 model:

Step by Step

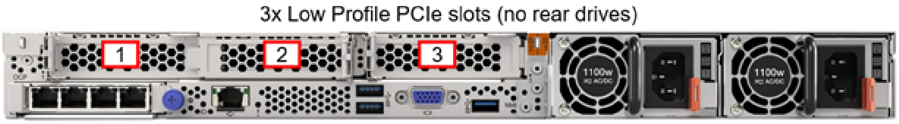
1) Refer to the Lenovo SR630 V2 rack installation instructions to install the server into the rack.

2) Install the disk drive.The image below shows the location of the two drives. The system comes with a total of up to 10 2.5-inch drive bays.


Front operator panel
2x USB ports (Port 1 for XCC)
External diagnostics port
Up to 10x 2.5-inch hot-swap drive bays (SAS/SATA, NVMe or AnyBay)
Also supports 4x 3.5-inch hot-swap drives (SAS/SATA or AnyBay) or 16x hot-swap EDSFF drive bays (NVMe)
Optional VGA port
Pull-out information tag

To remove a drive, slide the blue release latch to the right with one finger while using another finger to grasp the black drive handle and pull the hard disk drive out of the drive bay.

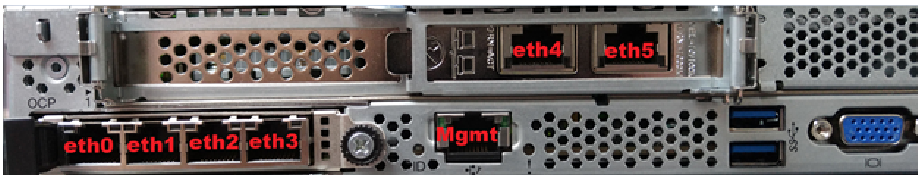
3) The image below gives a general overview of the connection panel in the rear of the Lenovo SR630 V2 server.



4) Installing the PCI.PCI installation is not required. The system comes pre-installed with six ports:

- ThinkSystem Broadcom 5719 1GbE RJ45 4-Port PCIe Ethernet Adapter (eth0 to eth3)
- ThinkSystem Broadcom 5720 1GbE RJ45 2-Port PCIe Ethernet Adapter (eth4 and eth5)

These are identified in the image below:



5) After adding and wiring all hardware to the machine, continue with the UEFI configuration and firmware updates. If you are using KVM devices connect it to the server prior to initial boot.

4 Installation and Upgrades Overview

This chapter describes the preparation of the USB stick and the installation, update or upgrade procedure of the OpenScape Session Border Controller software.

Administration and management of the OpenScape Session Border Controller is performed using an integrated and intuitive user GUI via a single point-of-entry using the same Common Management Platform (CMP) that is used to manage other components of the OpenScape Suite.

Installation and upgrades for OpenScape Session Border Controllers are currently performed via the same administration tools that are used for OpenScape Branch.

IMPORTANT: From V10, the open-vm-tools is installed in full install and the flag **Enable Open VM Tools** should be checked in System / Settings. If checked, this field enables the Open Virtual Machine Tools (open-vm-tools).

4.1 Installation and Upgrades

Preparation for installation, update or upgrade of the OpenScape Session Border Controller software:

Full Installation, Upgrades

Only one process for software delivery is supported: An entire image or a delta image that is used to rebuild a new image on the OpenScape Session Border Controller.

The following methods are available:

- **Full Installation**

  A new full installation erases both backup and active partition and overwrites them with software from the USB stick. This option is only available if the USB stick is plugged in and the system is booting from the USB stick.

  NOTICE: The database must be backed up to the USB stick, to preserve the data, prior to installation.

- **Upgrade OpenScape Session Border Controller software**:

  The system is upgraded using the concept of delta images. A full version will be installed on the backup partition and the active partition will be preserved in case of failure. Upgrade is possible using the USB stick or local files stored in PC/network. If the USB stick upgrade is performed only the files stored on the USB stick will be used, while in other methods the user has to choose which version will be used. The Software image *.tar file is required for all upgrades types. A tar file contains 3 files: `image*.ob, image*.key, and image*.sig`

- **Mass upgrades via CMP**:

  The following methods and tasks are supported:

  - Display a list of available software on the CMP (Common Management Platform) for downloading to the OpenScape Session Border Controller devices.
  - Software transfer or activation for a list of OpenScape Session Border Controller devices.
  - Software transfer of new software from the software repository or USB stick or remote locations to the CMP server.
  - Display a status overview of the software transfer or software activation process.
  - Scheduling multiple batches.

NOTICE: It is recommended to upgrade to the latest version of the current SBC software release before upgrading to a new SBC software release (i.e. from V9 to V10). Direct upgrade to V10R2 is allowed ONLY when OpenScape SBC system is running with V9R4.12.X or higher. In case of update/ upgrade failures, fallback to the backup partition and apply the recommended/tested upgrade path.

NOTICE: When upgrading OSBs or OS-SBC units to V10, the centralized OSB/OS-SBC license file needs to reflect the entire OSB/OS-SBC network and not just and individual OSB/OS-SBC that is being upgraded.

Software Images Provided for Customers

The following software is provided for customers on SWS (software repository).

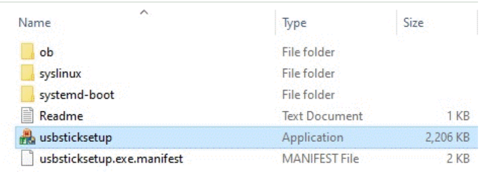
- **oss-10.02.*.*-*.zip**, that contains:
  - **image_oss-10.02.*.*-*.tar**– Software image file for upgrade or install.
  - **image_oss-10.02.*.*-*.spa**– File contains the compatibility information from the old release to new release for use by the CMP.
- **usbsticksetup_oss-10.02.*.*-*.zip**- Contains the USB Stick Wizard.
  - USB Stick Wizard
  - Installation file folders
- **misc_oss-10.02.*.*-*.tar.gz**- has the default XML configuration files and the MIBS.
- **vApps_oss-10.02.*.*-*.zip**- Contains the OVF templates to create and deploy a virtual machine for the various models of Virtual SBC.
- **oss-10.02.*.*-*.bz2**- Software image file for 4K Hosted.
- **sw-metadata-oss-10.02.*.*-*.json**- this file is used with OS Composer application.

NOTICE: Refer to USB Stick Setup Tool section (below) for example of folders and files included in the .zip file.

USB Stick Setup Tool

The USB Stick Wizard (usbsticksetup.exe) is a Windows application used to generate a USB Stick (pen drive) for OpenScape Session Border Controller Installation. This application is distributed with the following folders:

USB Stick Setup Folder (unzipped)



Name	Type	Size
ob	File folder	
syslinux	File folder	
systemd-boot	File folder	
Readme	Text Document	1 KB
usbsticksetup	Application	2,206 KB
usbsticksetup.exe.manifest	MANIFEST File	2 KB

4.1.1 How to Set Up the USB Stick

Proceed as follows to set up the USB stick for Installation:

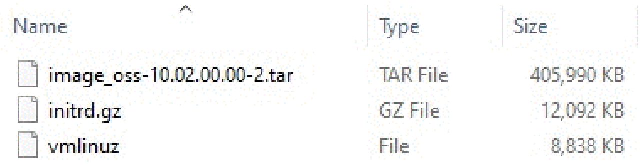
Prerequisites

One USB memory stick (minimum 2 GB memory capacity recommended).

The USB stick setup tool and the software image files are available on a local PC.

Step by Step

1) Extract the USB Stick Setup tool application from the zip file.
2) Copy the software image *.tar files into the ob folder. The folder will contain SW images for OpenScape Session Border Controller SW installation.



Name	Type	Size
image_oss-10.02.00.00-2.tar	TAR File	405,990 KB
initrd.gz	GZ File	12,092 KB
vmlinuz	File	8,838 KB

In this example, the base software file is *image_oss-10.02.00.00-2.tar* to be used for installing or upgrading.

3) Connect the USB stick to a USB port on the PC.
4) Proceed to the USB stick creation by running the usbsticksetup.exe application.

NOTICE: If doing a full installation using an existing DataBase (.xml), please make sure that the DB is exported from OpenScape Session Border Controller prior to start building the USB Stick. Via OpenScape SBC Assistant, select the **Import/Export** configuration menu and export the xml file. See Backup/Restore section in the OpenScape Voice Installation and upgrade Guide for more details. The exported config file will be selected in the following step under installation method as “Already existent database file”.

The **USB Stick Setup** screen is displayed.

5) In the **USB Stick Setup** screen:

a) In the Removable Media Select field, ensure that the USB stick is selected.

b) Select **Generate node.cfg file** to create a new configuration file. Network interfaces configuration is required with this option.

> **NOTICE:** If you select either the **Already existing database file or Already existing node.cfg file** option as the Installation Method the USB stick is created with data from the *.xml or *.cfg file you specify. With either option: the Host Name, IP Address, Subnet mask, and Default gateway (LAN only) fields are inactive (greyed out) and cannot be changed here. If you are using an *.xml or *.cfg as a template to install a new OpenScape Session Border Controller specific parameters will have to be specified or modified as necessary during the configuration process. The database file option can not be used for different hardware types.

c) In the **Host Name** field, enter a name for the system.

d) In the Network fields, specify the **IP Address, Subnet mask**, and **Default gateway** for the LAN/WAN Interfaces.

e) The **Partitioned USB Stick** field should be checked for Hardware servers.

f) From V10R2, the UEFI Bootloader option is available. By enabling this flag, the System Boot will be set as UEFI Mode. It is important that the server supports the UEFI Mode and then it is also configured to run in this mode.

g) Click **OK**.

A warning message is displayed: "All partitions of the removable media will be deleted and a single FAT32 partition will be created."

6) Click Yes to continue.

> **NOTICE:** After selecting **Yes** a warning will appear only if "image*.tar" is included in OpenScape Session Border Controller folder (OB folder). This is normal in cases where a full install is required and only the “image*.tar” is provided with the load. Click **Yes** to continue.

A progress bar is displayed.

7) When the USB Stick Setup tool indicates that “USB Stick setup complete”, click **OK**.

After the process is concluded the USB Stick can be removed and it will be ready for installation.

4.1.2 How to Update the Server Boot Sequence

The sever boot sequence may require update in order to perform a full installation of the OpenScape SBC software, if the server does not have the

USB storage as the first option for booting. Proceed as follows to update the server boot sequence.

Prerequisites

The server hardware has been installed e.g., IBM 3250 and IBM 3550.

The USB stick has been prepared.

NOTICE: After software installation, for security issues, it is recommended to start the boot from Hard Disk option.

Step by Step

1) Power on the server.

2) At boot up, wait and press **F1** to enter the BIOS setup when the option "<F1> Setup" is available.

The System Configuration and Boot Management window is displayed.

3) Use the **arrow key** to navigate to the "Boot Manager" and press **Enter**.

The Boot Management window is displayed.

4) Select **Add Boot Option** and press **Enter**.

5) Select **USB Storage** and press **Enter**.

6) Press **Esc** to exit and go back to the Boot Manager window.

The System Configuration and Boot Management window is displayed.

7) Select **Change Boot Order** and press **Enter**.

8) Press **Enter** again to change the order.

9) Using the "+" and "-" keys ensure the order is as follows: USB Storage, CD/DVD Rom, Hard Disk 0 and then press **Enter**.

The settings are temporarily saved.

10) Select **Commit Changes** to save the changes.

11) Press **Esc** to exit from all of the windows.

The prompt **Do you want to exit the Setup Utility?** is displayed.

12) When prompted with the message, select **Y**.

13) Once the Boot Sequence is updated, insert the USB stick and proceed with OpenScape SBC full installation.

The server boot sequence is updated and full installation of OpenScape SBC is now available. Proceed with USB full installation of OpenScape SBC software.

4.1.2.1 Boot device for one time use for IBM 3250M3/M5/M6 and 3550M3/M4/M5

IBM x3250M3/M5/M6, x3550M3/M4/M5 platforms

Step by Step

1) Plug in the USB stick to be used for the boot.

2) Power on or reboot the server.

3) When prompted, select **F12** to select Boot Device option.

4) In **Boot Devices Manager**, select **USB Storage** option.

5) Press **ESC** to exit.

4.1.2.1.1 Boot device for one time use for Lenovo SR250/SR250 V2, SR530 and SR630 V2

Lenovo SR530 , SR630 V2 and Lenovo SR250/SR250 V2 platforms

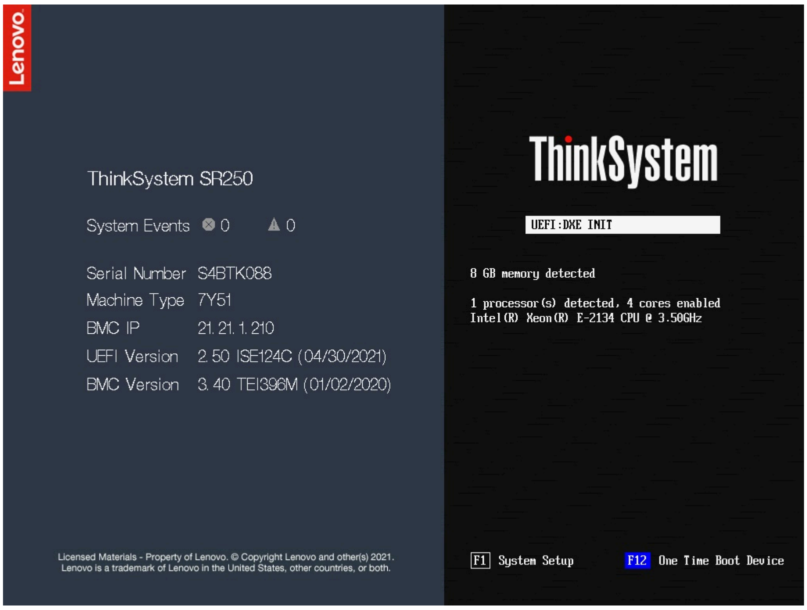
Step by Step

1) Plug in the USB stick to be used for the boot.

2) Power on or reboot the server.

3) When prompted, select F12 “One Time Boot Device” option.

SR250



Lenovo

ThinkSystem SR250

System Events ⊗ 0 ▲ 0

Serial Number S4BTK088
Machine Type 7Y51
BMC IP 21.21.1.210
UEFI Version 2.50 ISE124C (04/30/2021)
BMC Version 3.40 TEI396M (01/02/2020)

Licensed Materials - Property of Lenovo. © Copyright Lenovo and other(s) 2021.
Lenovo is a trademark of Lenovo in the United States, other countries, or both.

ThinkSystem

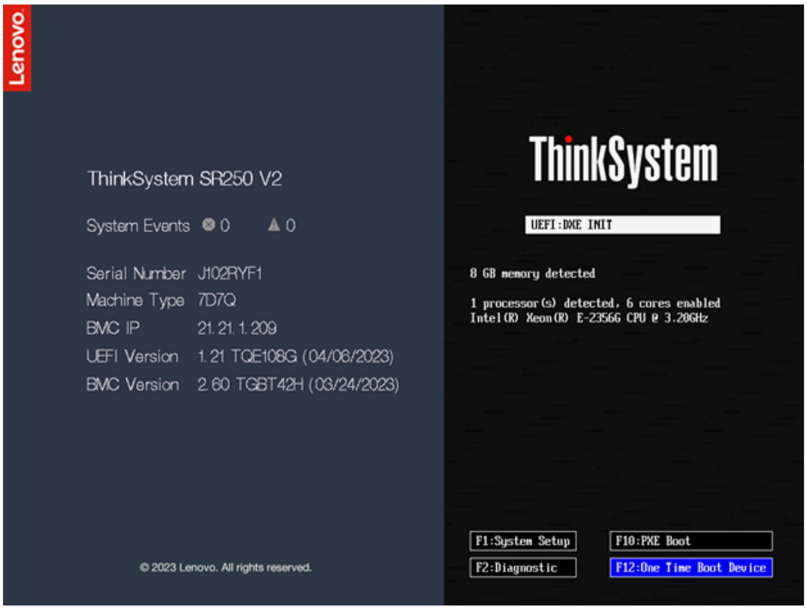
UEFI:DXE INIT

8 GB memory detected

1 processor(s) detected, 4 cores enabled
Intel(R) Xeon(R) E-2134 CPU @ 3.50GHz

F1 System Setup F12 One Time Boot Device

SR250 V2



Lenovo

ThinkSystem SR250 V2

System Events ⊗ 0 ▲ 0

Serial Number J102RYF1
Machine Type 7D7Q
BMC IP 21.21.1.209
UEFI Version 1.21 TQE108G (04/06/2023)
BMC Version 2.60 TGBT42H (03/24/2023)

© 2023 Lenovo. All rights reserved.

ThinkSystem

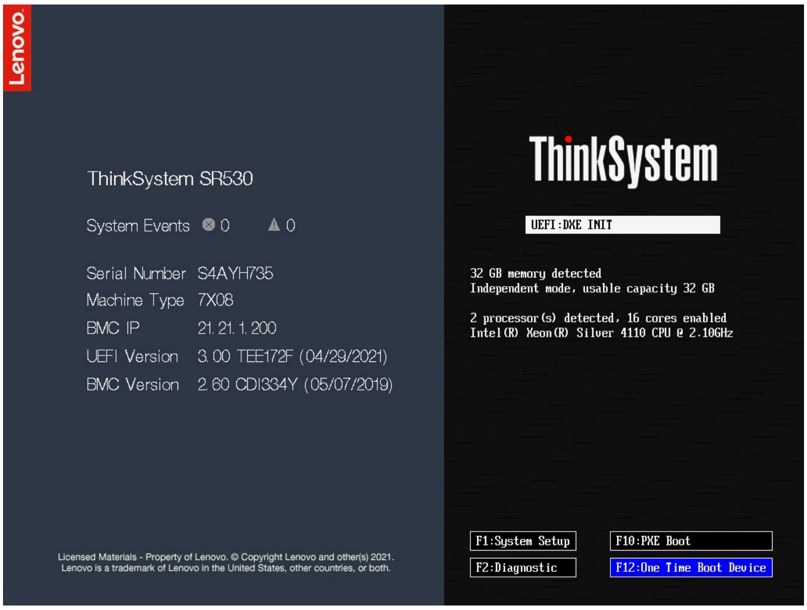
UEFI:DXE INIT

8 GB memory detected

1 processor(s) detected, 6 cores enabled
Intel(R) Xeon(R) E-2356G CPU @ 3.20GHz

F1:System Setup F10:PXE Boot
F2:Diagnostic F12:One Time Boot Device

SR530



ThinkSystem SR530

System Events ⊗ 0 ⚠ 0

```
Serial Number  S4AYH735
Machine Type   7X08
BMC IP         21.21.1.200
UEFI Version   3.00 TEE172F (04/29/2021)
BMC Version    2.60 CDI334Y (05/07/2019)
```

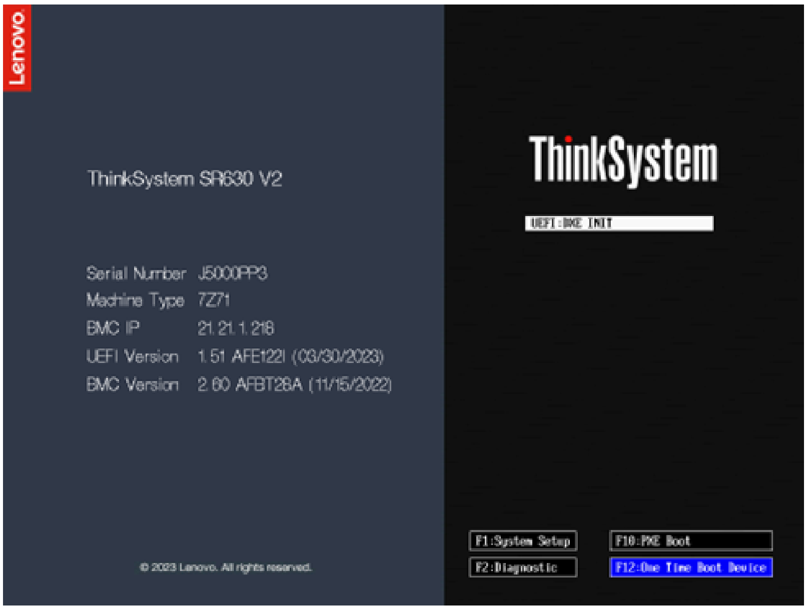
Licensed Materials - Property of Lenovo. © Copyright Lenovo and other(s) 2021.
Lenovo is a trademark of Lenovo in the United States, other countries, or both.

```
UEFI:DXE INIT

32 GB memory detected
Independent mode, usable capacity 32 GB

2 processor(s) detected, 16 cores enabled
Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
```

SR630 V2



ThinkSystem SR630 V2

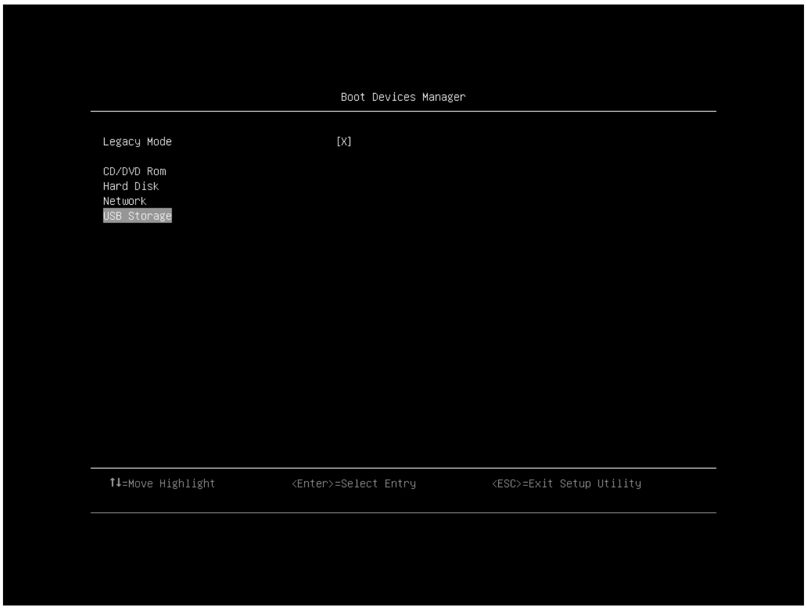
```
Serial Number  J5000PP3
Machine Type   7Z71
BMC IP         21.21.1.218
UEFI Version   1.51 AFE122I (03/30/2023)
BMC Version    2.60 AFBT28A (11/15/2022)
```

© 2023 Lenovo. All rights reserved.

```
UEFI:DXE INIT
```

4) In **Boot Devices Manager**, select the **USB Storage** option when the system is set as Legacy Mode or the **UEFI: USB** option when the system is set as UEFI Mode.

NOTICE: The name shown in the USB option in UEFI Mode changes depending on the brand/model of the USB:

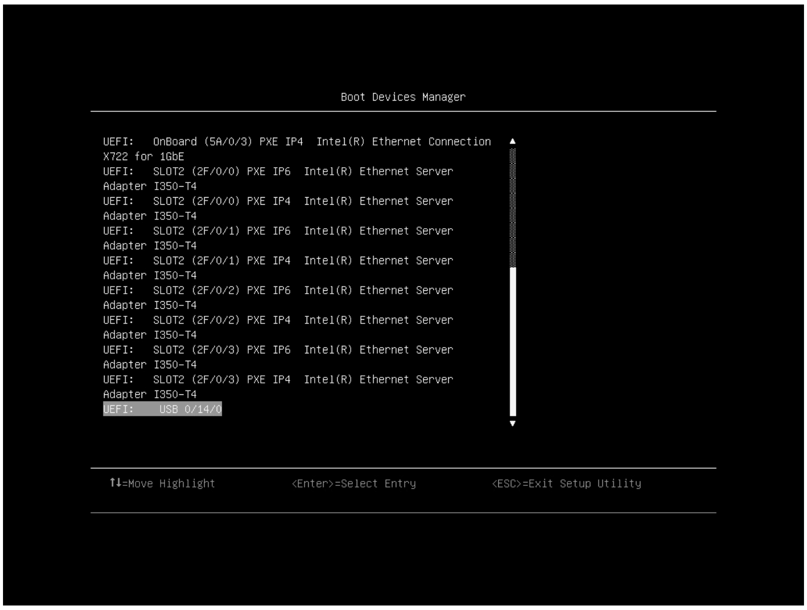


```
                         Boot Devices Manager
--------------------------------------------------------------------------

Legacy Mode                         [X]

CD/DVD Rom
Hard Disk
Network
USB Storage

--------------------------------------------------------------------------
  ↑↓=Move Highlight          <Enter>=Select Entry          <ESC>=Exit Setup Utility
--------------------------------------------------------------------------
```



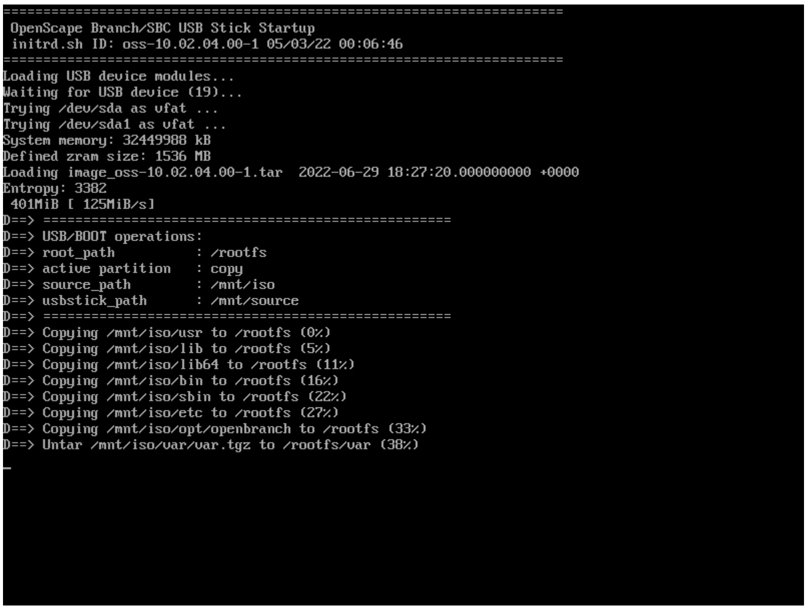
```
                         Boot Devices Manager
--------------------------------------------------------------------------

UEFI:   OnBoard (5A/0/3) PXE IP4  Intel(R) Ethernet Connection
X722 for 1GbE
UEFI:   SLOT2 (2F/0/0) PXE IP6  Intel(R) Ethernet Server
Adapter I350-T4
UEFI:   SLOT2 (2F/0/0) PXE IP4  Intel(R) Ethernet Server
Adapter I350-T4
UEFI:   SLOT2 (2F/0/1) PXE IP6  Intel(R) Ethernet Server
Adapter I350-T4
UEFI:   SLOT2 (2F/0/1) PXE IP4  Intel(R) Ethernet Server
Adapter I350-T4
UEFI:   SLOT2 (2F/0/2) PXE IP6  Intel(R) Ethernet Server
Adapter I350-T4
UEFI:   SLOT2 (2F/0/2) PXE IP4  Intel(R) Ethernet Server
Adapter I350-T4
UEFI:   SLOT2 (2F/0/3) PXE IP6  Intel(R) Ethernet Server
Adapter I350-T4
UEFI:   SLOT2 (2F/0/3) PXE IP4  Intel(R) Ethernet Server
Adapter I350-T4
UEFI:    USB 0/14/0

--------------------------------------------------------------------------
  ↑↓=Move Highlight          <Enter>=Select Entry          <ESC>=Exit Setup Utility
--------------------------------------------------------------------------
```

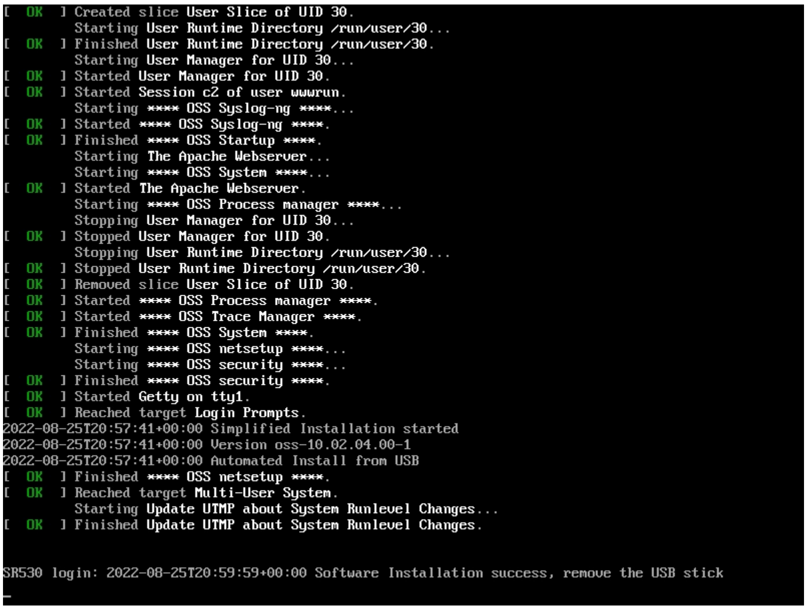
5) Press **Enter** to start the installation:

NOTICE: Automate installation or installation using GUI.



```
=====================================================================
 OpenScape Branch/SBC USB Stick Startup
 initrd.sh ID: oss-10.02.04.00-1 05/03/22 00:06:46
=====================================================================
Loading USB device modules...
Waiting for USB device (19)...
Trying /dev/sda as vfat ...
Trying /dev/sda1 as vfat ...
System memory: 32449988 kB
Defined zram size: 1536 MB
Loading image_oss-10.02.04.00-1.tar  2022-06-29 18:27:20.000000000 +0000
Entropy: 3382
 401MiB [ 125MiB/s]
D==> ====================================================
D==> USB/BOOT operations:
D==> root_path          : /rootfs
D==> active partition   : copy
D==> source_path        : /mnt/iso
D==> usbstick_path      : /mnt/source
D==> ====================================================
D==> Copying /mnt/iso/usr to /rootfs (0%)
D==> Copying /mnt/iso/lib to /rootfs (5%)
D==> Copying /mnt/iso/lib64 to /rootfs (11%)
D==> Copying /mnt/iso/bin to /rootfs (16%)
D==> Copying /mnt/iso/sbin to /rootfs (22%)
D==> Copying /mnt/iso/etc to /rootfs (27%)
D==> Copying /mnt/iso/opt/openbranch to /rootfs (33%)
D==> Untar /mnt/iso/var/var.tgz to /rootfs/var (38%)
_
```

6) After finishing the installation remove the USB stick before rebooting the system.



```
[  OK  ] Created slice User Slice of UID 30.
         Starting User Runtime Directory /run/user/30...
[  OK  ] Finished User Runtime Directory /run/user/30.
         Starting User Manager for UID 30...
[  OK  ] Started User Manager for UID 30.
[  OK  ] Started Session c2 of user wwwrun.
         Starting **** OSS Syslog-ng ****...
[  OK  ] Started **** OSS Syslog-ng ****.
[  OK  ] Finished **** OSS Startup ****.
         Starting The Apache Webserver...
         Starting **** OSS System ****...
[  OK  ] Started The Apache Webserver.
         Starting **** OSS Process manager ****...
         Stopping User Manager for UID 30...
[  OK  ] Stopped User Manager for UID 30.
         Stopping User Runtime Directory /run/user/30...
[  OK  ] Stopped User Runtime Directory /run/user/30.
[  OK  ] Removed slice User Slice of UID 30.
[  OK  ] Started **** OSS Process manager ****.
[  OK  ] Started **** OSS Trace Manager ****.
[  OK  ] Finished **** OSS System ****.
         Starting **** OSS netsetup ****...
         Starting **** OSS security ****...
[  OK  ] Finished **** OSS security ****.
[  OK  ] Started Getty on tty1.
[  OK  ] Reached target Login Prompts.
2022-08-25T20:57:41+00:00 Simplified Installation started
2022-08-25T20:57:41+00:00 Version oss-10.02.04.00-1
2022-08-25T20:57:41+00:00 Automated Install from USB
[  OK  ] Finished **** OSS netsetup ****.
[  OK  ] Reached target Multi-User System.
         Starting Update UTMP about System Runlevel Changes...
[  OK  ] Finished Update UTMP about System Runlevel Changes.


SR530 login: 2022-08-25T20:59:59+00:00 Software Installation success, remove the USB stick
_
```

4.1.2.1.2 Boot device for one time use for Fujitsu RX200 platforms

Fujitsu RX200 platforms

Step by Step

1) Plug in the USB stick to be used for the boot.

2) Power on or reboot the server.

3) At boot up wait and Press F2 to enter setup.

4) Use the right arrow to select the boot tab.

5) Select the USB as the boot option #1.

6) Exit setup.

7) Continue with the system boot.

> **NOTICE:** You can not select USB as a boot option since there are multiple USBs on the system, and picking a specific port would be problematic. The best solution is to plug a USB in (as shown below: a Kingston Data Traveler USBstick) and you can then select.

4.1.2.1.3 System Boot Mode - Legacy Mode or UEFI Mode

Before V10R2, only the Legacy Mode was available for system boot. Now, it is possible to choose the UEFI Mode to system boot.

> **NOTICE:** The System Boot Mode must be configured correctly, otherwise the Server will not boot from the Hard Drive.

Lenovo x3250M6 and x3550 M5 platforms

LEGACY MODE: Select F1 to enter in System Setup, choose Boot Manager option, the Boot Modes must be configured as Legacy Mode.

UEFI MODE: Select F1 to enter in System Setup, choose Boot Manager option, the Boot Mode must be changed to UEFI mode. In System Settings, the Legacy Support must be disabled.

Lenovo SR530, SR630 V2 and Lenovo SR250/SR250 V2 platforms

LEGACY MODE: Select F1 to enter in System Setup, choose UEFI Setup option, selects System Settings, the Legacy BIOS must be Enable. And the Boot Manager/Boot Modes must be configured as Legacy Mode.

UEFI MODE: Select F1 to enter in System Setup, choose UEFI Setup option, the Boot Manager/Boot Mode must be changed to UEFI mode. In System Settings, the Legacy BIOS must be disabled.

> **IMPORTANT:**

The following servers do not support UEFI Boot Mode:

Fujitsu Rx 200 S6

Fujitsu Rx 200 S7

For virtual machines, it is recommended to use Legacy Mode.

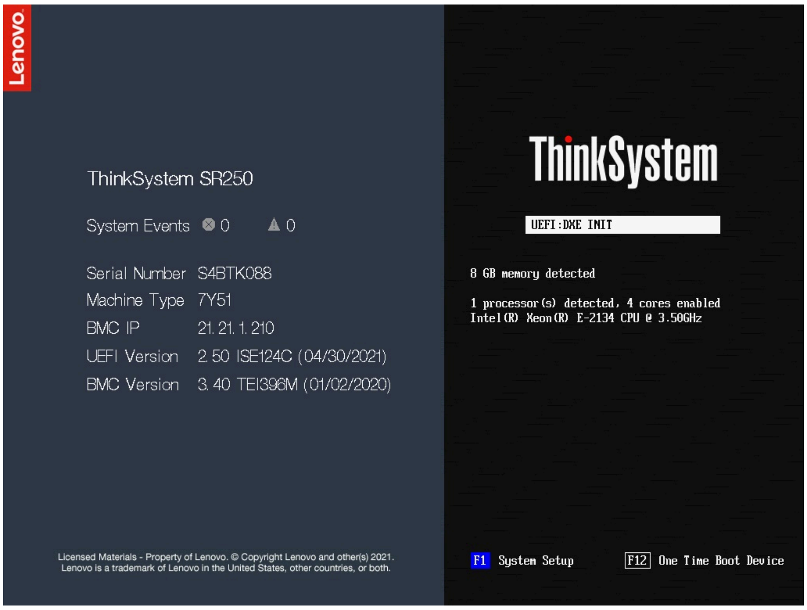
4.1.2.1.3.1 Lenovo SR250/SR250 V2, Lenovo SR530 and Lenovo SR630 V2 platforms- Legacy Mode

Before V10R2, only the Legacy Mode was available for system boot. Now, it is possible to choose the UEFI Mode to system boot (see).

Step by Step

1) Select F1 to enter in System Setup:

SR250



ThinkSystem SR250

System Events ⊗ 0 ▲ 0

Serial Number S4BTK088
Machine Type 7Y51
BMC IP 21.21.1.210
UEFI Version 2.50 ISE124C (04/30/2021)
BMC Version 3.40 TEI396M (01/02/2020)

Licensed Materials - Property of Lenovo. © Copyright Lenovo and other(s) 2021.
Lenovo is a trademark of Lenovo in the United States, other countries, or both.

ThinkSystem

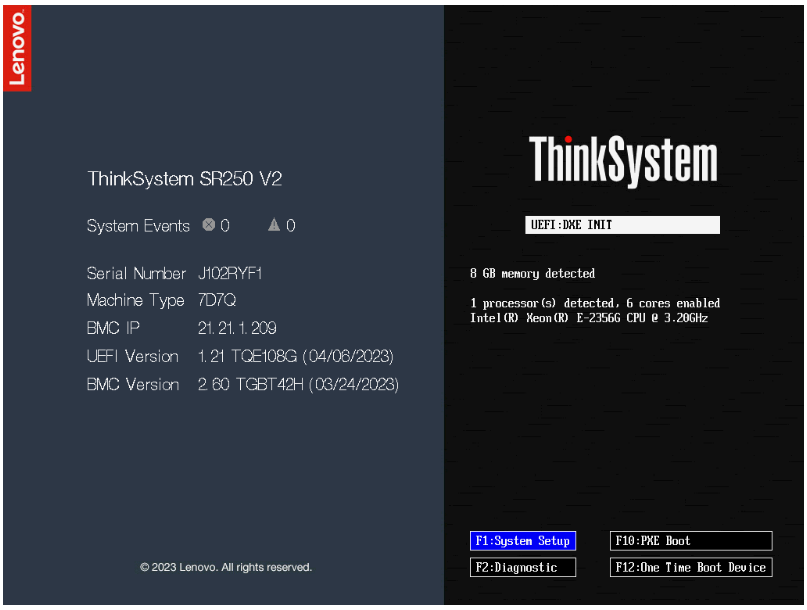
UEFI:DXE INIT

8 GB memory detected

1 processor(s) detected, 4 cores enabled
Intel(R) Xeon(R) E-2134 CPU @ 3.50GHz

F1 System Setup F12 One Time Boot Device

SR250 V2



ThinkSystem SR250 V2

System Events ⊗ 0 ▲ 0

Serial Number J102RYF1
Machine Type 7D7Q
BMC IP 21.21.1.209
UEFI Version 1.21 TQE108G (04/06/2023)
BMC Version 2.60 TGBT42H (03/24/2023)

© 2023 Lenovo. All rights reserved.

ThinkSystem

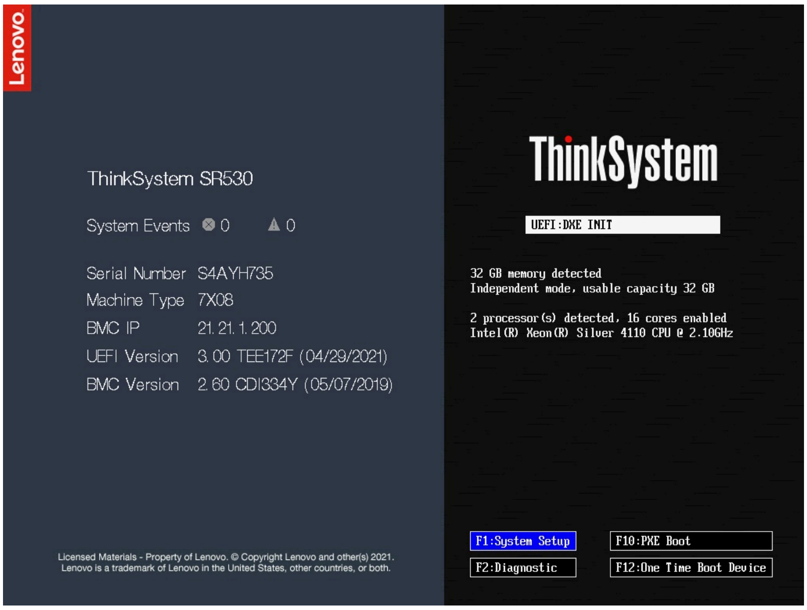
UEFI:DXE INIT

8 GB memory detected

1 processor(s) detected, 6 cores enabled
Intel(R) Xeon(R) E-2356G CPU @ 3.20GHz

F1:System Setup F10:PXE Boot
F2:Diagnostic F12:One Time Boot Device

SR530



ThinkSystem SR530

System Events ⊗ 0 ▲ 0

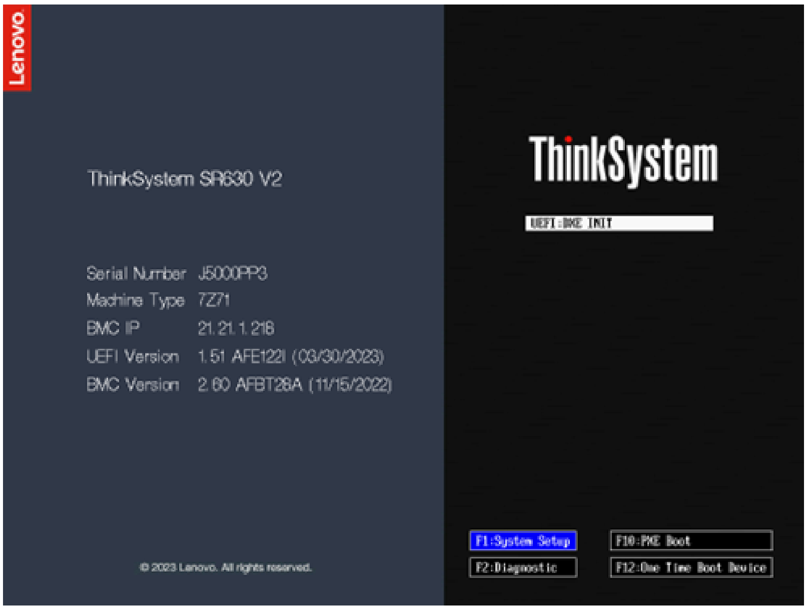
Serial Number S4AYH735
Machine Type 7X08
BMC IP 21.21.1.200
UEFI Version 3.00 TEE172F (04/29/2021)
BMC Version 2.60 CDI334Y (05/07/2019)

Licensed Materials - Property of Lenovo. © Copyright Lenovo and other(s) 2021.
Lenovo is a trademark of Lenovo in the United States, other countries, or both.

```
32 GB memory detected
Independent mode, usable capacity 32 GB

2 processor(s) detected, 16 cores enabled
Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
```

SR630 V2



ThinkSystem SR630 V2

Serial Number J5000PP3
Machine Type 7Z71
BMC IP 21.21.1.216
UEFI Version 1.51 AFE122I (03/30/2023)
BMC Version 2.60 AFBT28A (11/15/2022)

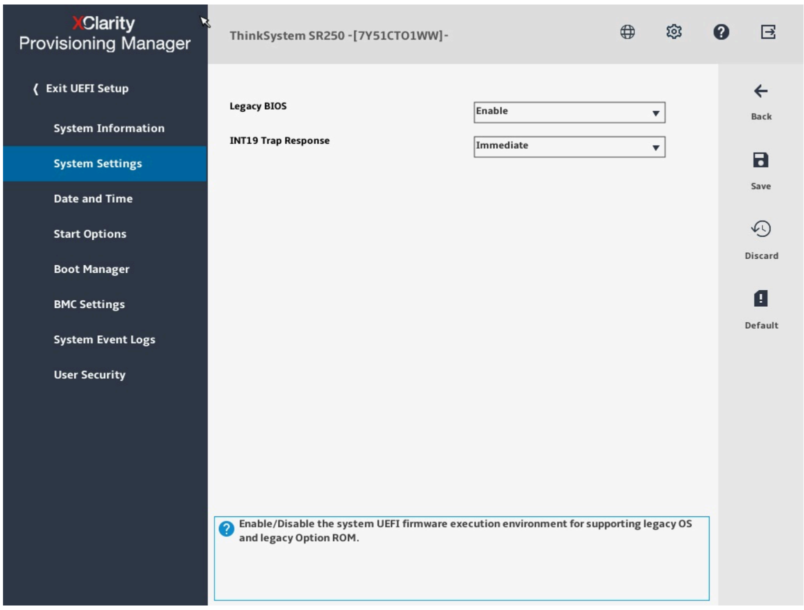
© 2023 Lenovo. All rights reserved.

2) Select **UEFI Setup**.

3) Select **System Settings**.

NOTICE: The **Legacy BIOS** must be enabled and the **Boot Manager/Boot Modes** must be configured as **Legacy Mode**.

SR250

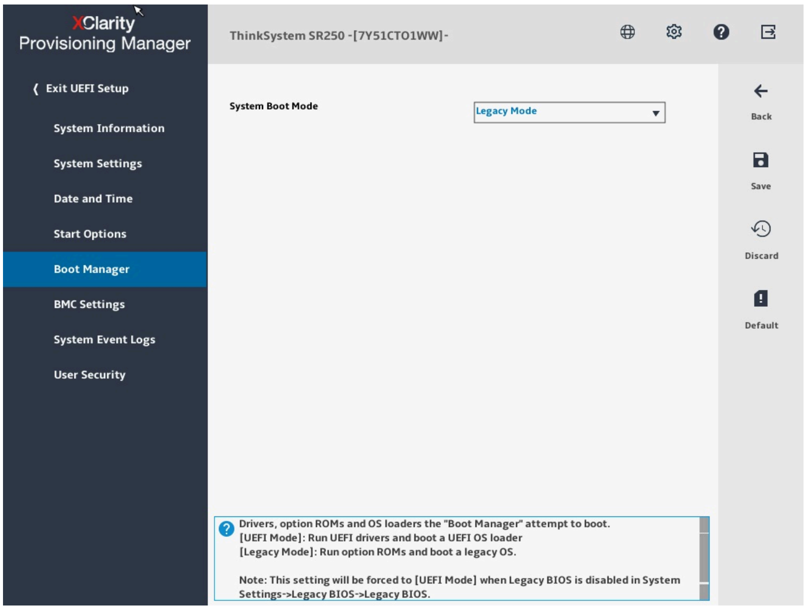


ThinkSystem SR250 -[7Y51CTO1WW]-

Legacy BIOS: Enable

INT19 Trap Response: Immediate

Enable/Disable the system UEFI firmware execution environment for supporting legacy OS and legacy Option ROM.



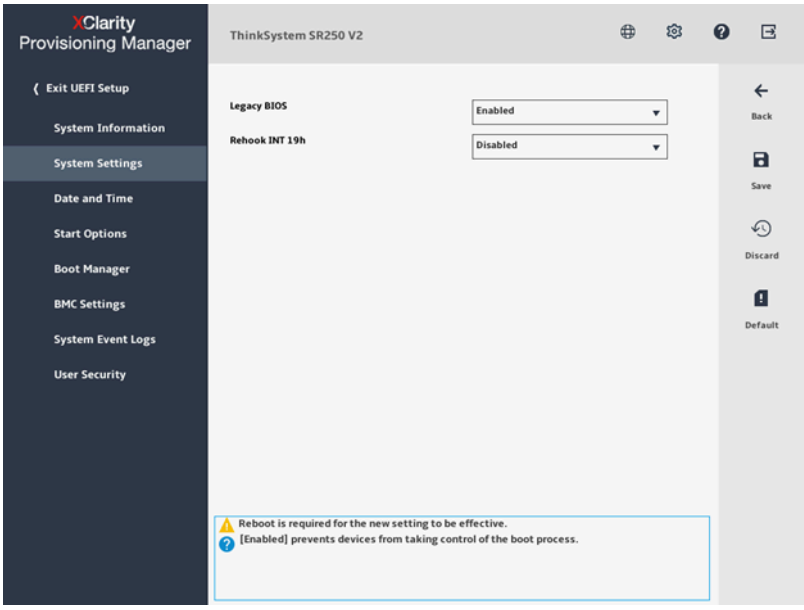
ThinkSystem SR250 -[7Y51CTO1WW]-

System Boot Mode: Legacy Mode

Drivers, option ROMs and OS loaders the "Boot Manager" attempt to boot.
[UEFI Mode]: Run UEFI drivers and boot a UEFI OS loader
[Legacy Mode]: Run option ROMs and boot a legacy OS.

Note: This setting will be forced to [UEFI Mode] when Legacy BIOS is disabled in System Settings->Legacy BIOS->Legacy BIOS.

SR250 V2

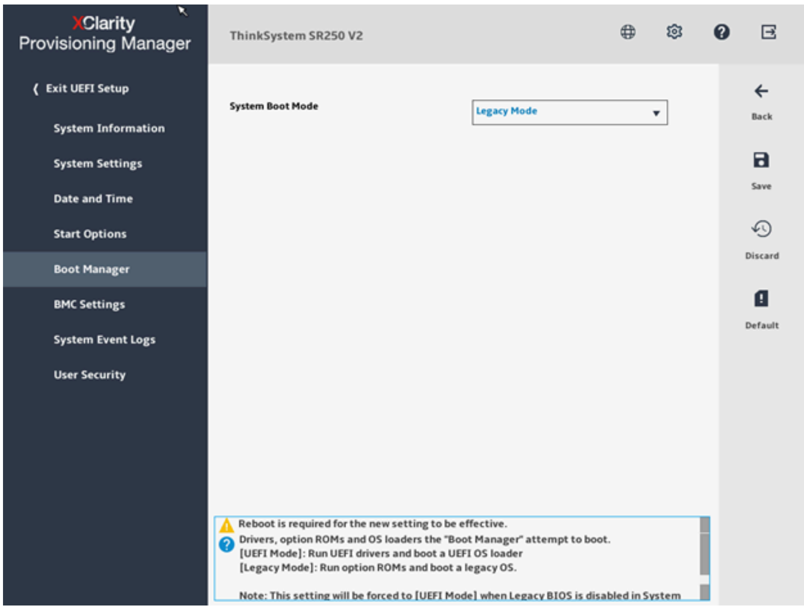


Legacy BIOS: Enabled

Rehook INT 19h: Disabled

Reboot is required for the new setting to be effective.
[Enabled] prevents devices from taking control of the boot process.

SR250 V2

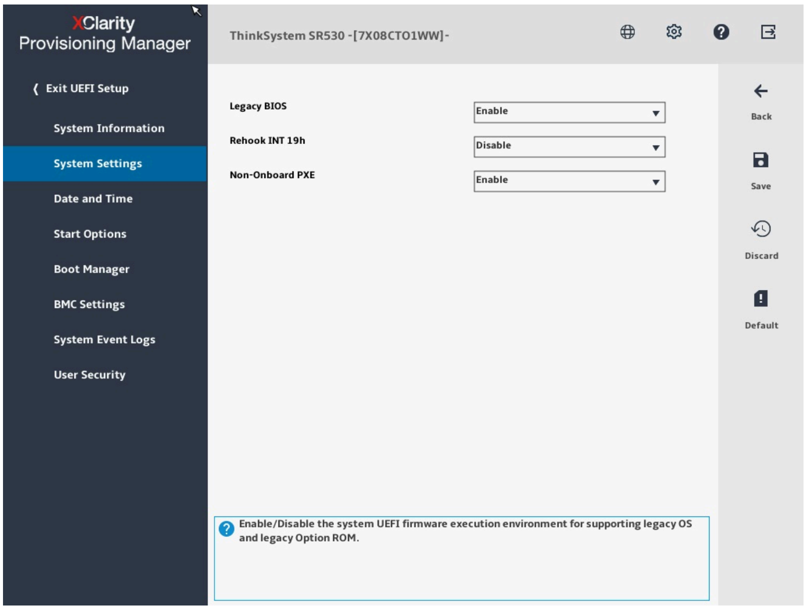


System Boot Mode: Legacy Mode

Reboot is required for the new setting to be effective.
Drivers, option ROMs and OS loaders the "Boot Manager" attempt to boot.
[UEFI Mode]: Run UEFI drivers and boot a UEFI OS loader
[Legacy Mode]: Run option ROMs and boot a legacy OS.

Note: This setting will be forced to [UEFI Mode] when Legacy BIOS is disabled in System

SR530



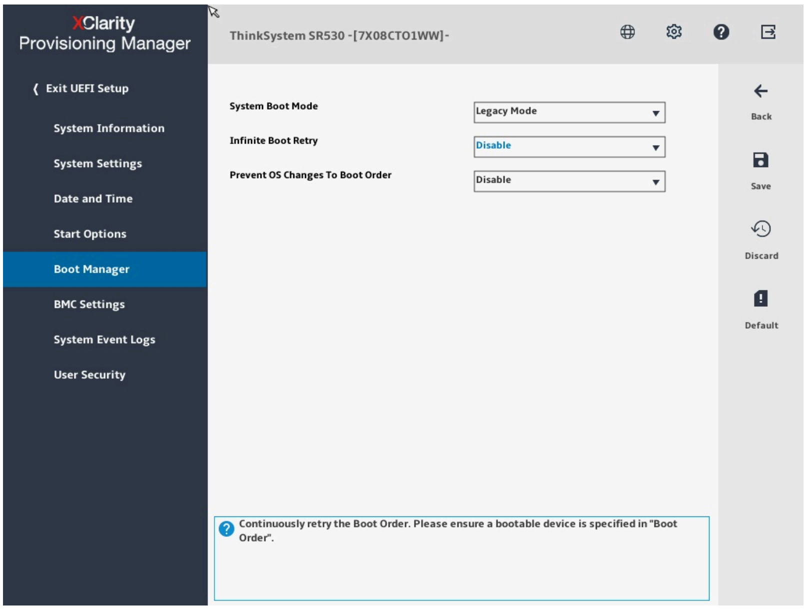
ThinkSystem SR530 -[7X08CTO1WW]-

Legacy BIOS: Enable

Rehook INT 19h: Disable

Non-Onboard PXE: Enable

Enable/Disable the system UEFI firmware execution environment for supporting legacy OS and legacy Option ROM.



ThinkSystem SR530 -[7X08CTO1WW]-

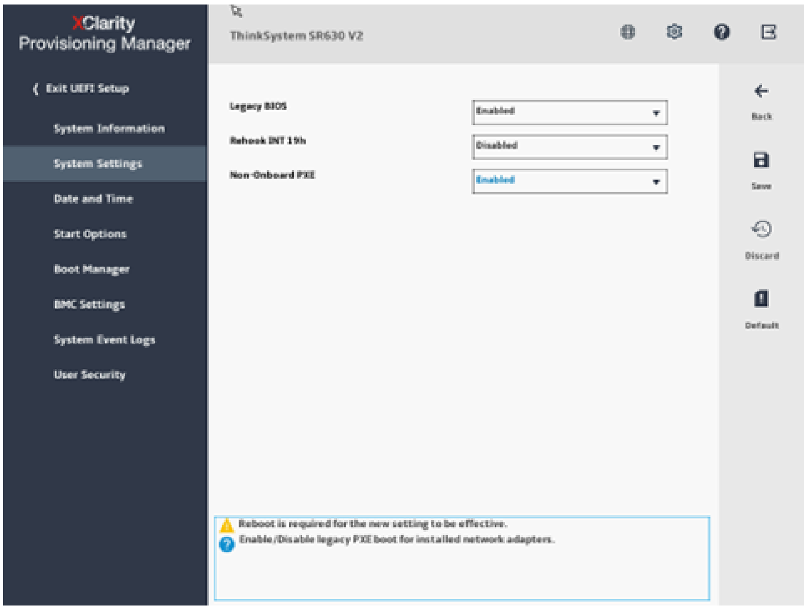
System Boot Mode: Legacy Mode

Infinite Boot Retry: Disable

Prevent OS Changes To Boot Order: Disable

Continuously retry the Boot Order. Please ensure a bootable device is specified in "Boot Order".

SR630 V2



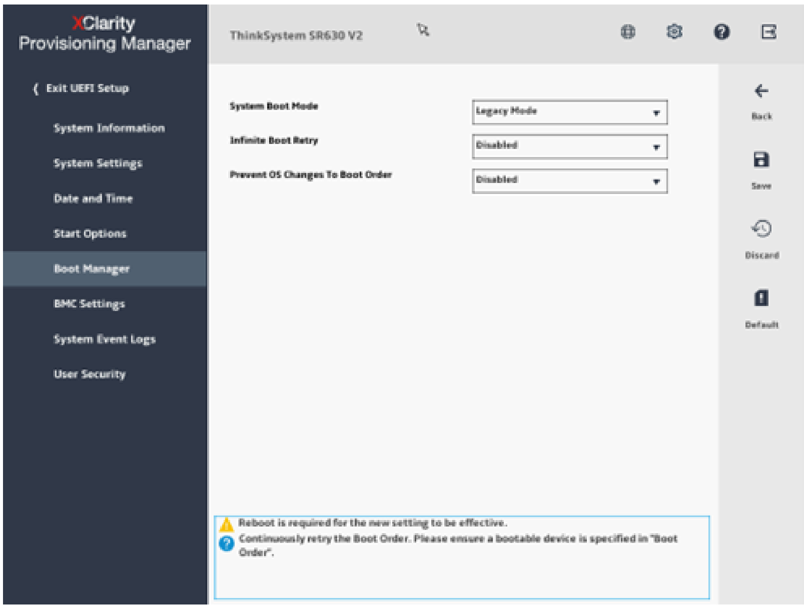
Legacy BIOS: Enabled

Rehook INT 19h: Disabled

Non-Onboard PXE: Enabled

Reboot is required for the new setting to be effective.

Enable/Disable legacy PXE boot for installed network adapters.



System Boot Mode: Legacy Mode

Infinite Boot Retry: Disabled

Prevent OS Changes To Boot Order: Disabled

Reboot is required for the new setting to be effective.

Continuously retry the Boot Order. Please ensure a bootable device is specified in "Boot Order".

4) Save the changes before Exit.

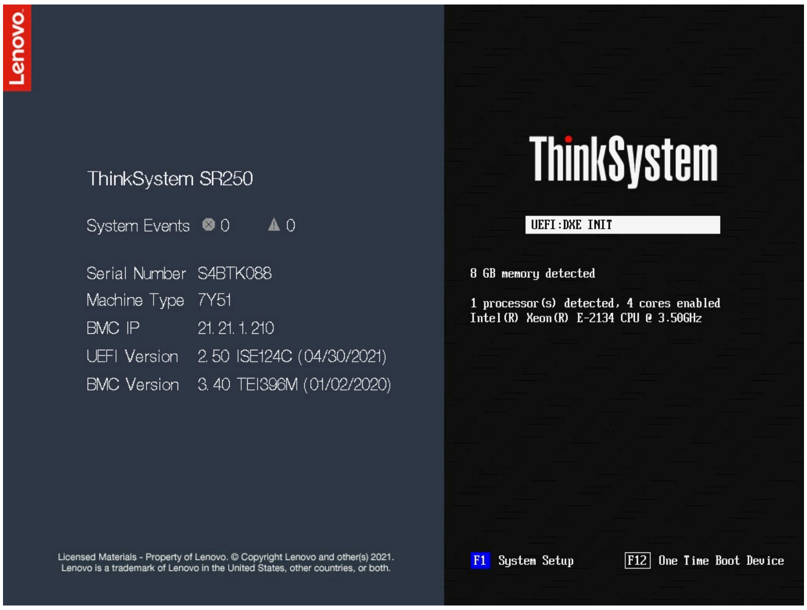
4.1.2.1.3.2 Lenovo SR250/SR250 V2, Lenovo SR530 and Lenovo SR630 V2 platforms- UEFI Mode

Before V10R2, only the Legacy Mode was available for system boot. Now, it is possible to choose the UEFI Mode to system boot.

Step by Step

1) Select F1 to enter in System Setup:

SR250



ThinkSystem SR250

System Events ⊗ 0 ▲ 0

Serial Number S4BTK088
Machine Type 7Y51
BMC IP 21.21.1.210
UEFI Version 2.50 ISE124C (04/30/2021)
BMC Version 3.40 TEI396M (01/02/2020)

Licensed Materials - Property of Lenovo. © Copyright Lenovo and other(s) 2021.
Lenovo is a trademark of Lenovo in the United States, other countries, or both.

ThinkSystem

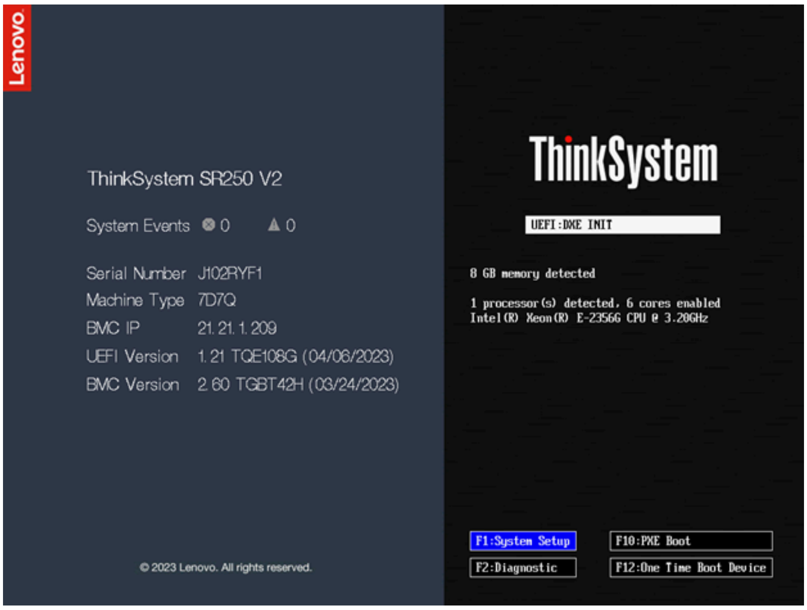
```
UEFI:DXE INIT

8 GB memory detected

1 processor(s) detected, 4 cores enabled
Intel(R) Xeon(R) E-2134 CPU @ 3.50GHz

F1 System Setup          F12 One Time Boot Device
```

SR250 V2



ThinkSystem SR250 V2

System Events ⊗ 0 ▲ 0

Serial Number J102RYF1
Machine Type 7D7Q
BMC IP 21.21.1.209
UEFI Version 1.21 TQE108G (04/06/2023)
BMC Version 2.60 TGBT42H (03/24/2023)

© 2023 Lenovo. All rights reserved.

ThinkSystem

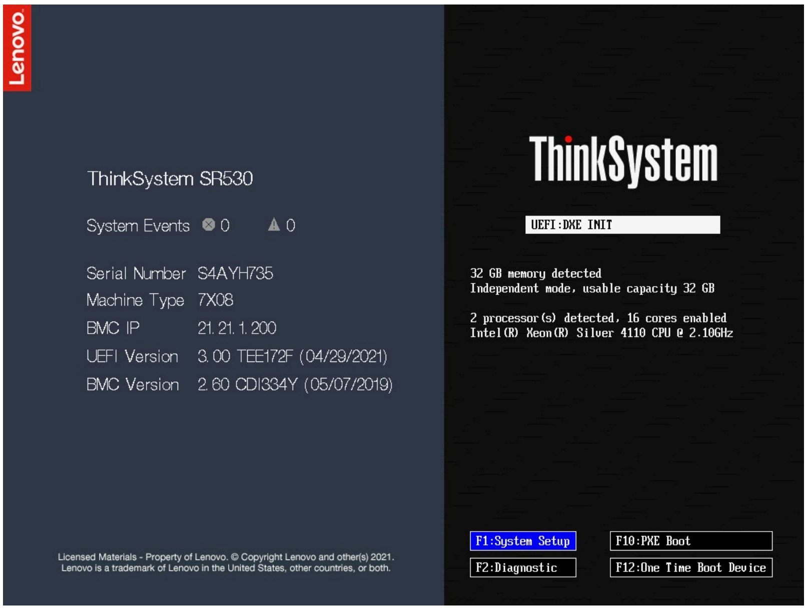
```
UEFI:DXE INIT

8 GB memory detected

1 processor(s) detected, 6 cores enabled
Intel(R) Xeon(R) E-2356G CPU @ 3.20GHz

F1:System Setup          F10:PXE Boot
F2:Diagnostic            F12:One Time Boot Device
```

SR530



ThinkSystem SR530

System Events ⊗ 0 ▲ 0

```
Serial Number  S4AYH735
Machine Type   7X08
BMC IP         21.21.1.200
UEFI Version   3.00 TEE172F (04/29/2021)
BMC Version    2.60 CDI334Y (05/07/2019)
```

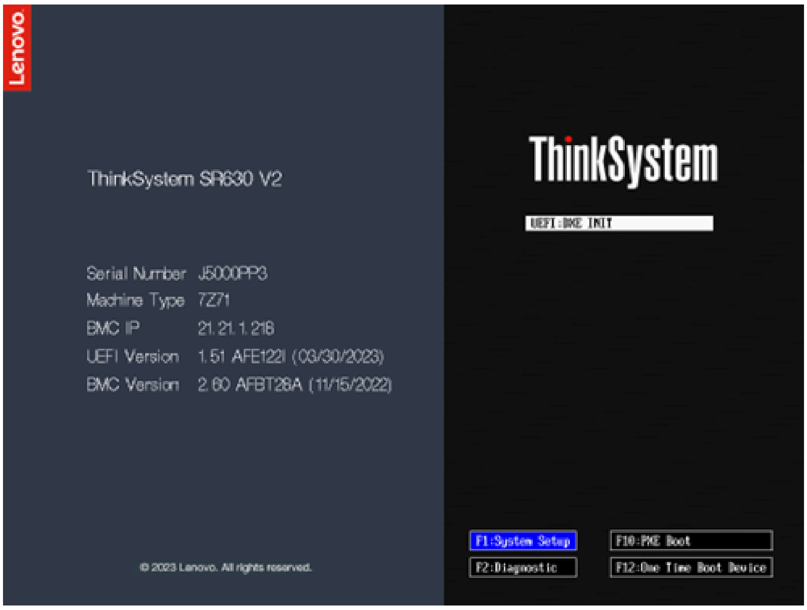
```
UEFI:DXE INIT

32 GB memory detected
Independent mode, usable capacity 32 GB

2 processor(s) detected, 16 cores enabled
Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
```

Licensed Materials - Property of Lenovo. © Copyright Lenovo and other(s) 2021.
Lenovo is a trademark of Lenovo in the United States, other countries, or both.

SR630 V2



ThinkSystem SR630 V2

```
Serial Number  J5000PP3
Machine Type   7Z71
BMC IP         21.21.1.218
UEFI Version   1.51 AFE122I (03/30/2023)
BMC Version    2.60 AFBT28A (11/15/2022)
```

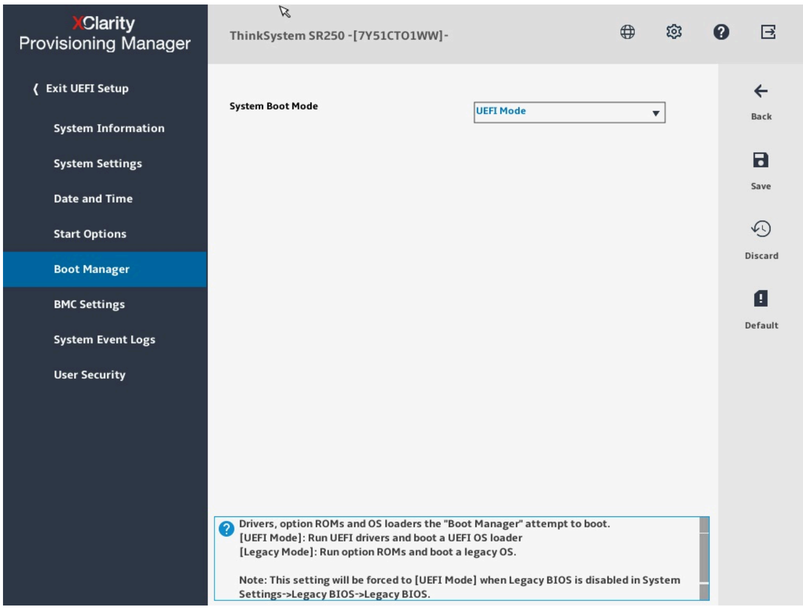
```
UEFI:DXE INIT
```

© 2023 Lenovo. All rights reserved.

2) Select **UEFI Setup**.

NOTICE: Boot Manager/Boot Mode must be changed to UEFI mode. In System Settings, the **Legacy BIOS** must be disabled.

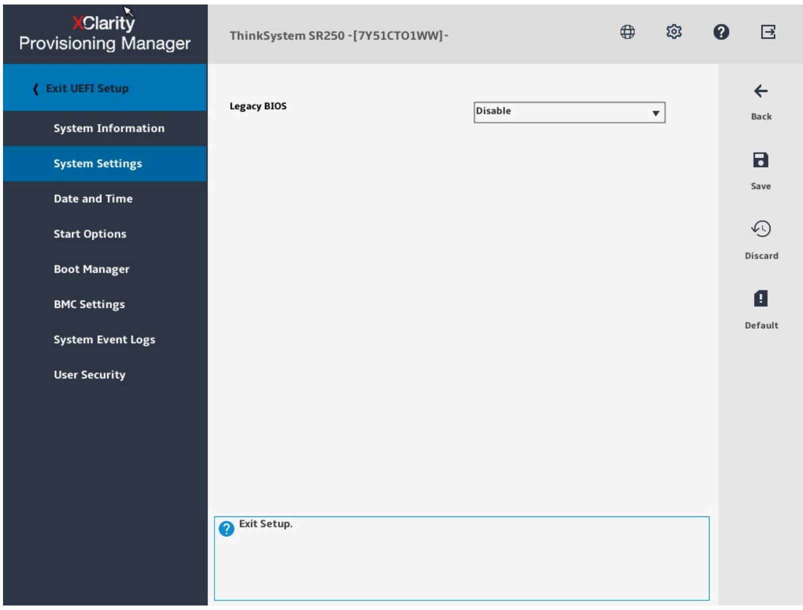
SR250



System Boot Mode: UEFI Mode

Drivers, option ROMs and OS loaders the "Boot Manager" attempt to boot.
[UEFI Mode]: Run UEFI drivers and boot a UEFI OS loader
[Legacy Mode]: Run option ROMs and boot a legacy OS.

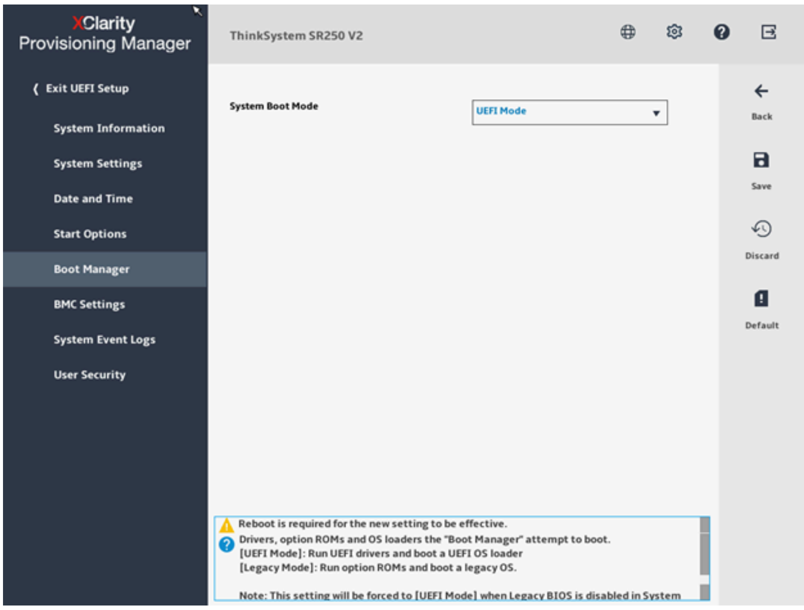
Note: This setting will be forced to [UEFI Mode] when Legacy BIOS is disabled in System Settings->Legacy BIOS->Legacy BIOS.



Legacy BIOS: Disable

Exit Setup.

SR250 V2

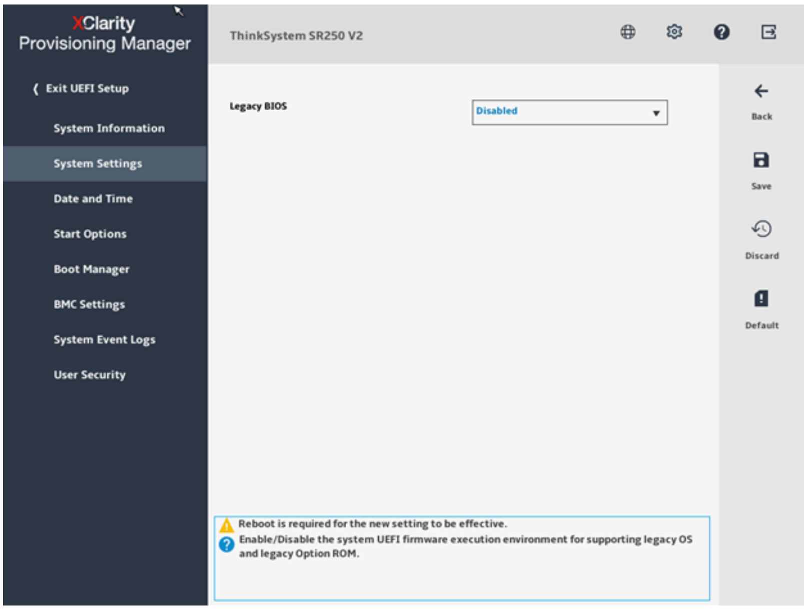


System Boot Mode: UEFI Mode

Reboot is required for the new setting to be effective.
Drivers, option ROMs and OS loaders the "Boot Manager" attempt to boot.
[UEFI Mode]: Run UEFI drivers and boot a UEFI OS loader
[Legacy Mode]: Run option ROMs and boot a legacy OS.

Note: This setting will be forced to [UEFI Mode] when Legacy BIOS is disabled in System

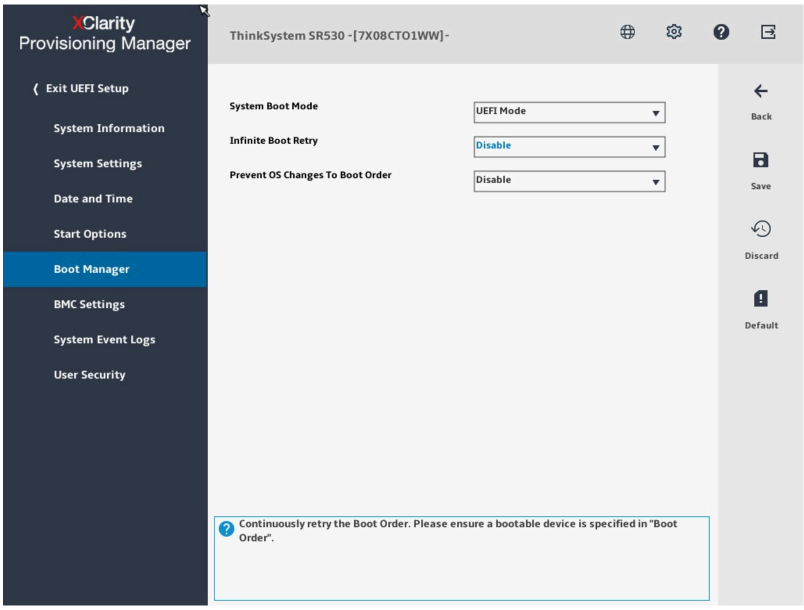
SR250 V2



Legacy BIOS: Disabled

Reboot is required for the new setting to be effective.
Enable/Disable the system UEFI firmware execution environment for supporting legacy OS and legacy Option ROM.

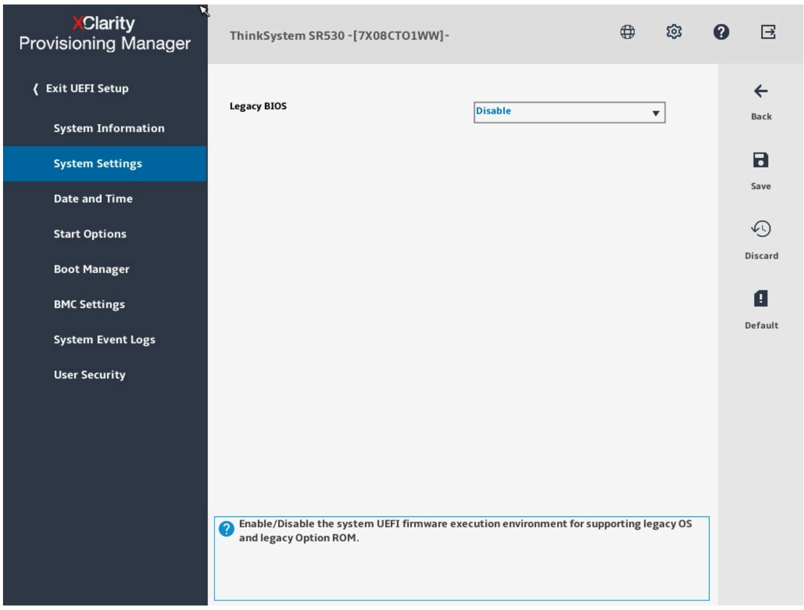
SR530



ThinkSystem SR530 -[7X08CTO1WW]-

System Boot Mode	UEFI Mode
Infinite Boot Retry	Disable
Prevent OS Changes To Boot Order	Disable

Continuously retry the Boot Order. Please ensure a bootable device is specified in "Boot Order".

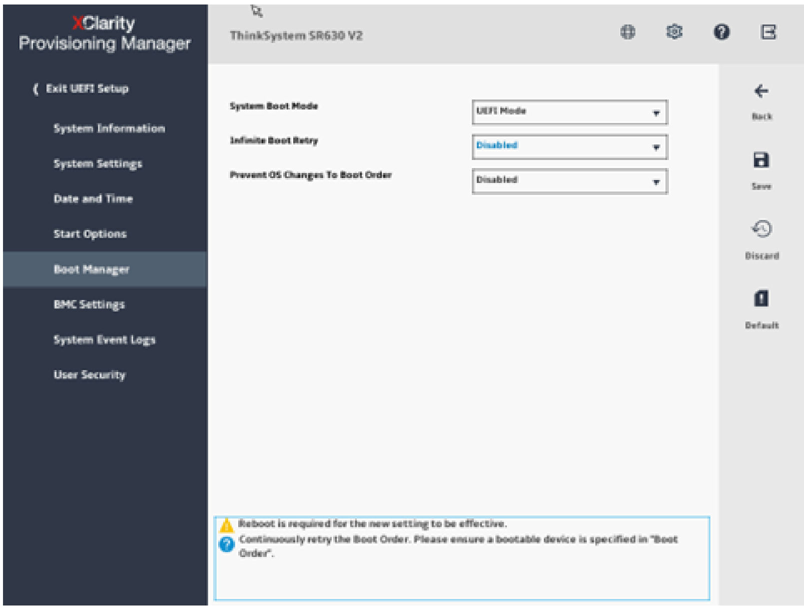


ThinkSystem SR530 -[7X08CTO1WW]-

Legacy BIOS	Disable

Enable/Disable the system UEFI firmware execution environment for supporting legacy OS and legacy Option ROM.

SR630 V2



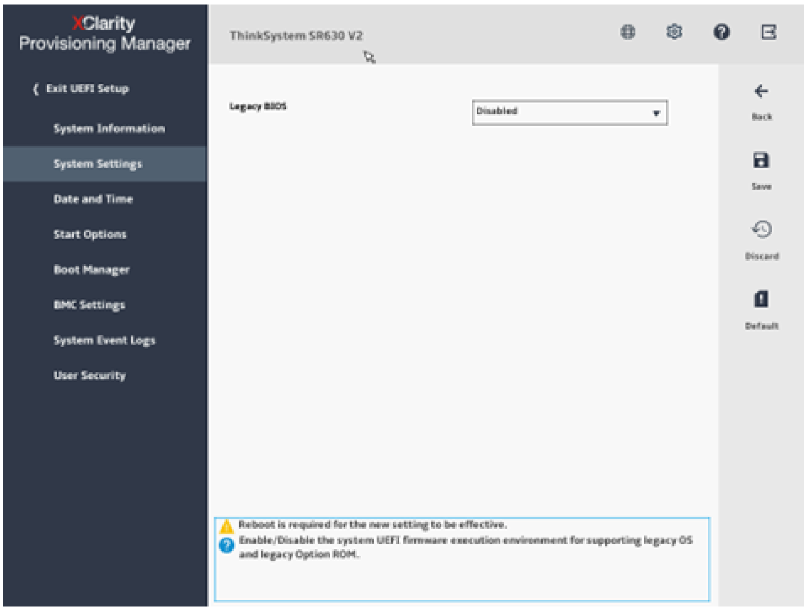
System Boot Mode: UEFI Mode

Infinite Boot Retry: Disabled

Prevent OS Changes To Boot Order: Disabled

Reboot is required for the new setting to be effective.

Continuously retry the Boot Order. Please ensure a bootable device is specified in "Boot Order".



Legacy BIOS: Disabled

Reboot is required for the new setting to be effective.

Enable/Disable the system UEFI firmware execution environment for supporting legacy OS and legacy Option ROM.

3) Save the changes before Exit.

4.1.3 How to Perform a Full Installation of the OpenScape Session Border Controller Software

Proceed as follows to install the OpenScape Session Border Controller software on the server. This procedure is performed using the OpenScape Session Border Controller Management Portal (local GUI); it is not supported from the Common Management Platform (CMP) because the OpenScape Session Border Controller application first requires an IP address be assigned and discovered.

Prerequisites

The server hardware has been installed.

The USB stick has been prepared.

Step by Step

1) Connect the USB stick you created to a USB port on the server and restart the server. Press F12 to SR250/SR250 V2/SR530/SR630 V2 servers to select the USB stick drive.

> **NOTICE:** The Installation erases both backup and active partitions and overwrites them with existent SW in USB.

2) Open an internet browser and enter the OpenScape Session Border ControllerLAN IP address (defined previously with the OpenScape Session Border ControllerUSB Stick Setup tool) via https:// in the Address field).

> **NOTICE:** From V10R2, the Local GUI is optimized for current versions of Chrome, Edge and Firefox. Please note that using IE or other browsers may lead to rendering errors and/or limited.
>
> The Edge browser appears to render some colors differently than Chrome and Firefox, for example some check box controls in Edge may appear grayer than the blue check mark controls rendered in Firefox and Chrome.

The OpenScape Session Border Controller Management Portal login screen is displayed.

3) Log in to the OpenScape Session Border Controller Management Portal with User name: administrator and Password: Asd123!. (note the period [dot] at the end).

4) After you are logged in, you will be alerted that “You are booting from USB stick”. Click **OK**.

The **OpenScape SBC** tab is displayed.

5) Select the **Maintenance** > **Install / Upgrade** > **Installation menu** and click **Install**(the Installation option is only shown when booting from USB stick).

> **NOTICE:** From V10R1, there is a new option to select the number of code partitions to be created. The default is 2 (one for the active version and other for the backup version). From now, it is possible to have until 5 partitions of code. Despite the number of partitions selected, the number created can be below due to the disk size limitations. For instance: you can select 5, but just 3 will be created.

> **NOTICE:** From V10R2, the UEFI bootloader flag is available in the installation option. A “UEFI Bios detected” or “UEFI Bios NOT detected” message is shown. The UEFI bootloader flag could be activated in the USBsticksetup. Please, make sure to choose this option. The System Boot

Mode must be configured correctly, otherwise the Server will not boot from the Hard Drive.

NOTICE: All previous data in the system will be lost. If USB stick was created with a Config/DB file then that will be applied during installation.

6) When prompted to confirm that you want to perform a full installation, click **OK**.

   The installation will begin and takes about 15 minutes for an OpenScape Session Border Controllersystem. A progress bar shows the percent complete for the installation process.

7) When prompted with the message, “System installed. Press OK to reboot the system now”, click **OK**.

8) When prompted to “Please remove the USB stick before continue”, remove the USB stick and click **OK**.

   The system will boot in about three minutes.

9) Open an internet browser and enter the OpenScape Session Border ControllerIP address (defined previously with the OpenScape Session Border USB Stick Setup tool) via https:// in the Address field.

   NOTICE: No configuration changes are allowed for about 5-10 minutes while the process manager checks if the system is stable.

   The installation is checked and a information message is displayed: "The process manager is working to ensure that the system is stable. Please wait a few minutes and try again."

10) Click **OK** to confirm the message. At this point the user may use the Local GUI or Common Management Platform (CMP) for configuration.

If the check of the installation fails, the system will reboot to the backup partition; in the case of a full installation and both partitions are failing then a re-installation is required.

4.1.4 How to Upgrade OpenScape Session Border Controller Software via the CMP Software Repository

Proceed as follows to upgrade an OpenScape Session Border Controller using the CMP Software Repository.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

The connection to the CMP Software Repository is up.

Step by Step

1) Select the **Maintenance**, tab followed by the **Inventory** button, and then select **Repository in the Navigation Tree**.

   The system presents the **Software Repository** work area displays a list of software and version number.

   > **NOTICE:** Note that effective with OpenScape SBC V8 the software versions use the’Fit4more’ format. For example,
   >
   > 10.01.05.01-1 (V10 R1.5.1)
   >
   > 10.02.00.00-2 (V10 R2.0.0)

2) To add a software image to the CMP Software Repository select the **Add** button.

   The **Add to software repository** window opens.

3) Click the **Browse** button to select and upload file.

   The **Choose File to Upload** dialog opens.

4) Click the **Open** button to complete the file selection. Select the **image_oss-*.*.*.*-*.spa** and then the **image_oss-*.*.*.*-*.tar** files.

   The **Add to software repository** window is displayed with the selected file.

5) Click the **Save** button to upload the selected files.

   Software is now added and ready to be used for Upgrades/Updates.

6) In the Common Management Platform (CMP), select the **Maintenance**, tab followed by the **Inventory** button, and then select **Applications in the Navigation Tree**.

   The system presents the **Applications** form with a current list of all applications.

7) In the row of the respective OpenScape Session Border Controller application, select the **Software activation** command.

   The **Software activation** dialog appears.

8) Select **Common Repository** in the **Location** selection list.

9) Select the file version to be activated from the **Version** selection list.

   > **NOTICE:** Only applicable images are displayed in the list.

10) Click the **Activate...** button to activate the software as displayed in the list. The activation may take some time.

    The **Software activation - Current status** window appears.

    > **NOTICE:** The **Software activation - Current status** window may not be closed until the status "completed" is displayed in the window.

11) Click the **Close** button.

The software is activated at the OpenScape Session Border Controller and the Software activation window is closed.

4.1.5 How to Upgrade OpenScape Session Border Controller Software via USB Stick

Proceed as follows to upgrade an OpenScape Session Border Controller using a software image stored on an USB stick.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

The connection to the Common Management Platform (CMP) is up.

Step by Step

1) Connect the USB stick you created to an USB port.

2) In the Common Management Platform (CMP), select the **Maintenance**, tab followed by the **Inventory** button, and then select **Applications in the Navigation Tree**.

The system presents the **Applications** form with a current list of all applications.

3) In the row of the respective OpenScape Session Border Controller application, select the **Software activation** command by clicking the arrow on the right hand side of the work area followed by clicking the **Software Activation** button.

The **Software activation** dialog appears.

4) Select **USB stick** in the **Location** selection list. The following options are available:

5) Select the file version to be activated from the **Version** selection list.

NOTICE: Only applicable images are displayed in the list.

6) Click the **Activate...** button to activate the software as displayed in the list. The activation may take some time.

The **Software activation - Current status** window appears.

NOTICE: The **Software activation - Current status** window may not be closed until the status "completed" is displayed in the window.

7) Click the **Close** button.

The action is completed.

4.1.6 How to Upgrade OpenScape Session Border Controller Software via Local GUI

Proceed as follows to upgrade an OpenScape Session Border Controller using a Local GUI.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape SBC system is up.

> **NOTICE:** Before performing a local file/SFTP/HTTPS upgrade, place the IP address of the server where the new software image is into the Message Rate Control White List.

Step by Step

1) Navigate to SBC LOCAL GUI> Security> Message Rate Control White List.
2) Type the IP address and click **Add** and **Apply Changes**.

> **NOTICE:** From V10R2, the Local GUI is optimized for current versions of Chrome, Edge and Firefox. Please note that using IE or other browsers may lead to rendering errors and/or limited. The Edge browser appears to render some colors differently than Chrome and Firefox, for example some check box controls in Edge may appear grayer than the blue check mark controls rendered in Firefox and Chrome.

4.1.6.1 Software source as USB stick

Step by Step

1) Access the OpenScape SBC using Local GUI or CMP. The USB stick has been prepared and connected in the system.
2) Select **Maintenance**>**Install/Upgrade**>**Upgrade** option.
3) In **Software Source** choose the option to upgrade: **USB stick**.
4) After receiving the message to Upgrade from USB stick, select **OK** .
5) After the process is completed, a **System upgraded** message is displayed. Click **OK**.
6) The messages **A new version is ready to be activated** and **Please remove the USB stick before continuing** are displayed. Click OK.
   The software version is shown in **New Code Activation**.
7) Click **Activate now** to activate the software.

   The messages **Do you want to reboot the system and activate the software now?** and **WARNING!!! It could NOT wait for active calls be disconnected** are displayed. Click **OK** to restart the system.
8) it is possible to **Abandon** or **Remove** the installed software. The **Abandon** button removes the new flag from the new partition and avoids pop-ups saying that a new version is ready to be activated. It can be still selected as

the new software version in the **Restart** tab. The **Remove** button sets it as cleared and it makes it unavailable for usage.

4.1.6.2 Software source as Local file

Step by Step

1) Access the OpenScape SBC using Local GUI or CMP. The USB stick has been prepared and connected in the system.

2) Select **Maintenance**>**Install/Upgrade**>**Upgrade** option.

3) In **Software Source** choose the option to upgrade: **Local file**.

4) Choose the file stored in Computer or stored in the local network.

5) Click **Upgrade**.

The file is uploaded and the message **File(s) uploaded** is displayed. Click **OK**.

6) The message **Are you sure you want to upgrade from local file(s)?** is displayed. Click **OK**.

7) After the completion of the process, the message **System upgrated** is displayed. Click **OK**.

8) The message **A new version is ready to be activated** is displayed. Click **OK**.

The software version is shown in **New Code Activation**.

9) Click **Activate now** to activate the software.

The messages **Do you want to reboot the system and activate the software now?** and **WARNING!!! It could NOT wait for active calls be disconnected** are displayed. Click **OK** to restart the system.

10) it is possible to **Abandon** or **Remove** the installed software. The **Abandon** button removes the new flag from the new partition and avoids pop-ups saying that a new version is ready to be activated. It can be still selected as the new software version in the **Restart** tab. The **Remove** button sets it as cleared and it makes it unavailable for usage.

4.1.6.3 Software source as SFTP

Step by Step

1) Access the OpenScape SBC using Local GUI or CMP.

2) Select **Maintenance** > **Install/Upgrade**> **Upgrade** option.

3) In **Software Source** choose the option to upgrade: **SFTP**.

4) Save the **oss_image-*.*.*.*-*.tar** file inrespective directory in **SFTP server**. Create the file **list** without extension in the same directory. Add the version name in this list, for instance: image_oss-10.02.00.00-2.tar.

5) Enter the following information: **Hostname** (ip address or fqdn), **Port** (22), **Remote directory**, **User name** and **Password**. The information related to SFTP server.

6) Click **List Versions**.

7) Choose the desired version in **Software version** option. The files that are in the **list** file are listed.

8) Click **Upgrade**.

   The file is downloaded and the message **File(s) downloaded** is displayed. Click **OK.**

9) The message **Are you sure you want to upgrade from SFTP?** is displayed. Click **OK**.

10) After the process is completed, the message **System upgraded** is displayed. Click **OK**.

11) The message **A new version is ready to be activated** is received. Click **OK**.

    The software version is shown in **New Code Activation**.

12) Click **Activate now** to activate the software.

    The messages **Do you want to reboot the system and activate the software now?** and **WARNING!!! It could NOT wait for active calls be disconnected** are displayed. Click **OK** to restart the system.

13) it is possible to **Abandon** or **Remove** the installed software. The **Abandon** button removes the new flag from the new partition and avoids pop-ups saying that a new version is ready to be activated. It can be still selected as the new software version in the **Restart** tab. The **Remove** button sets it as cleared and it makes it unavailable for usage.

4.1.6.4 Software source as HTTPS

Step by Step

1) Access the OpenScape SBC using Local GUI or CMP.

2) Select **Maintenance** > **Install/Upgrade**> **Upgrade** option.

3) In **Software Source** choose the option to upgrade: **HTTPS**.

4) Save the **oss_image-*.*.*.*-*.tar** and **oss_image-*.*.*.*-*spa** files inrespective directory in **HTTPS server**. Create the file **list** without extension in the same directory. Add the version name in this list, for instance: image_oss-10.02.00.00-2.tar.

5) Enter the following information: **Hostname** (ip address or fqdn) and **Remote directory**. The information related to HTTPS server.

6) Click **List Versions**.

7) Choose the desired version in **Software version** option. The files that are in the **list** file are listed.

8) Click **Upgrade**.

   The file is downloaded and the message **File(s) downloaded** is displayed. Click **OK**.

9) The message **Are you sure you want to upgrade from HTTPS?** is displayed. Click **OK**.

10) After the process is completed, the message **System Upgrated** is displayed. Click **OK**.

11) The message **A new version is ready to be activated** is displayed. Click **OK**.

    The software version is shown in **New Code Activation**.

12) Click **Activate now** to activate the software.

    The messages **Do you want to reboot the system and activate the software now?** and **WARNING!!! It could NOT wait for active calls be disconnected** are displayed. Click **OK** to restart the system.

13) it is possible to **Abandon** or **Remove** the installed software. The **Abandon** button removes the new flag from the new partition and avoids pop-ups saying that a new version is ready to be activated. It can be still selected as the new software version in the **Restart** tab. The **Remove** button sets it as cleared and it makes it unavailable for usage.

4.2 Virtualization - Overview

This chapter describes the preparation for installation of the OpenScape Session Border Controller in a virtual environment.

Testing of Virtual Solution

Tests have been executed for an OpenScape SBC virtual solution. For configuration details, see Section Virtual Machine Configuration Parameters.

Test Environment 1 employed the following:

- **ESXi 6.0/6.5/6.7/7.0 Virtual Machine running on x3550 M3/M4/M5** (same as native hardware).

NOTICE:

The x3550 M3/M4/M5 contains 12 GB Ram and a 300 GB HD to cover VMware overhead.

- 8 CPUs – (2 quad core processors minimum 2.5 GHZ)
- 8 GB RAM
- 140GB HD
- 2 NW adapters

Resource Reservation settings:

- CPU – Shares = High
- CPU – Reservation = 20000 MHz
- CPU – Limit = 20000 MHz
- Memory – Shares = Normal
- Memory – Reservation = 8 GB
- Memory – Limit = 8 GB
- Amount of virtual processors = 8
- HD = 140GB
- Hyper threading = off
- CPU Affinity = off

Characteristics of the Virtual OpenScape SBC

The virtual OpenScape SBC has the following characteristics.

- Is HW independent
- Hardware sensing and monitoring is disabled when configuring OpenScape SBC as virtual. Percentage of CPU, Memory and Disk usage will still be

reported and alarmed (e.g., CPU usages too high) and reflect the usage of the virtual machine. Statistics can be viewed in the **Maintenance** tab> **Inventory** > **Nodes** > **Dashboard for the system**.

- Currently supports and requires a fixed number of 2 (virtual) Ethernet ports
- Supports a 2 node clustering with each OpenScape Voice node.
- OpenScape SBC cluster can be co-located on 1 ESXi host for Software redundancy and 2 ESXi hosts for hardware redundancy. It can use internal or SAN storage.
- OpenScape SBC is compatible with ESXi V6.0/6.5/6.7/7.0 and all hardware used must be on the VMware compatibility list for ESXi V6.0/6.5.6.7/7.0.
- Supports failover to a second OpenScape SBC node.

Disk Space Limitations:

If you choose to install from an ISO image file instead of a DVD, please allocate at least 5 GB of disk space in a node’s datastore for the placement of the Virtualization Image DVD ISO and Node Configuration files

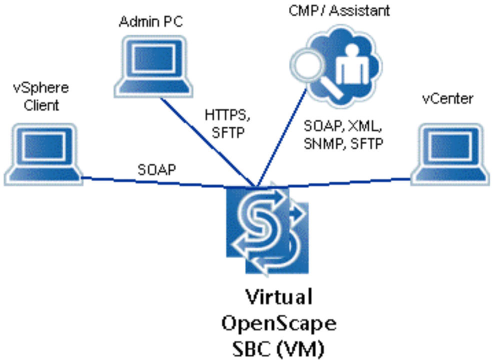
Other Limitations:

The virtual OpenScape SBC system is hardware (HW) independent. It is assumed that the HW platform is installed, supervised and maintained by the customer. This includes the installation and configuration of the virtual machine that will host the OpenScape SBC.

The virtual OpenScape SBC assumes it has one disk and 2 virtual Ethernet ports.

VM Management

VMware ESXi vSphere Client/Host Client provides the interface to vCenter and to the ESXi server where the Virtualized OpenScape SBC is running.



Backup/Restore database versus VM snapshots

It is recommended to use OpenScape SBC Backup and Restore databases procedures instead of VM snapshots. It is not recommended to use VM Snapshots in a production environment except during initial installation process. All Snapshots should be removed once the OpenScape SBC VM is placed into production.

4.2.1 Virtual Machine Configuration Parameters

This provides the configuration parameters needed to configure each OpenScape Session Border Controller in a virtual environment.

For more details, see OpenScape Solution Set V10, OpenScape Virtual Machine Resourcing and Configuration Guide.

VM resources for OpenScape SBC

The following table values shall be used to set the VM resources.

Deployment	Virtual OSS 250	Virtual OSS 6000	Virtual OSS 20000
Deployment Scenario	Single or redundant node	Single or redundant node	Single or redundant node
Nodes	1-2 active-standby	1-2 active-standby	1-2 active-standby
Users (See VMware Metrics)	<=250 (registrations)	<=6000 (registrations)	<=20,000 (registrations)
Server	Each SBC node	Each SBC node	Each SBC node
Guest OS	OpenSUSE 15.3 (configure as "Other 2.6x Linux (64-Bit)")	OpenSUSE 15.3 (configure as "Other 2.6x Linux (64-Bit)")	OpenSUSE 15.3 (configure as "Other 2.6x Linux (64-Bit)")
Realtime Application Note:Resources need to be reserved for Real time apps otherwise availability cannot be guaranteed	Y	Y	Y
IOPS – Input/output operations per second (Storage I/O) Note from VMware Resource Management Guide: Before using Storage I/O Control on data stores that are backed by arrays with automated storage tiering capabilities, check the VMware Storage/SAN Compatibility Guide to verify whether your automated tiered storage array has been certified to be compatible with Storage I/O Control.	7 I/O per second actual usage	20 I/O per second actual usage	30 I/O per second actual usage
Disk Throughput in KBps	100 KB/sec	400 KB/sec	600 KB/sec
Network Bandwidth in KBps	Core (eth0): 100 KB/sec.; Access (eth1): 16,000 KB/sec	Core (eth0): 500 KB/sec.; Access (eth1): 60,000 KB/sec	Core (eth0): 1000 KB/sec.; Access (eth1): 120,000 KB/sec

Deployment	Virtual OSS 250	Virtual OSS 6000	Virtual OSS 20000
Number of Virtual Disks	1	1	1
Virtual Disk Size	40 GB	40 GB	60 GB
Virtual disk mode The Virtual disk mode setting “independent” disallows the creation of Snapshots of a virtual machine. For a customer environment; it is recommended the Mode settings are NOT selected. This is the default configuration. Mode Independent Persistent will leave changes permanently written to disk Mode Independent Non-persistent writes data to disk but the data will be eliminated on restart (good for a training or demo environment)	Use defaults (Snapshot)	Use defaults (Snapshot)	Use defaults (Snapshot)
Virtual disk format type Note: using thick eager-zeroed virtual disk reduces delays the first time that a block is written to the disk and ensures that all space is allocated and initialized at creation time.Note: FT requires thin disk to be converted to thick eager-zeroed	Thick lazy-zeroed	Thick lazy-zeroed	Thick lazy-zeroed
Additional HD space needed (on the server/ SAN) to hold things like images, patchsets, mass provisioning files, restore cd, etc	5 GB	5 GB	5 GB
vCPU	2 1 virtual socket	4 2 virtual sockets	8 2 virtual sockets
vCPU Shares H=High N=Normal	High	High	Custom Configure "Custom" to reach 20,000MHz. "H" allows maximum 16,000MHz.
vCPU Reservation	5,000 MHz	10,000 MHz	20,000 MHz
vCPU Limit	5,000 MHz	10,000 MHz	20,000 MHz

Deployment	Virtual OSS 250	Virtual OSS 6000	Virtual OSS 20000
VM Memory [GB]***	4 GB	4 GB	6 GB
VVM Memory Shares H = High N = Normal***	N	N	N
VM Memory Reservation***	4 GB	4 GB	6 GB
VM Memory Limit***	4 GB	4 GB	6 GB
# vNICs (Note ****)	2	2	2
VMware manual MAC used [Y/N]	Y - Only for Local license file	Y - Only for Local license file	Y - Only for local license file
VMware VMotion supported [Y/N] (Note *)	Y (V7 and later)	Y (V7 and later)	Y (V7 and later)
VMware High Availability supported [Y/N]	Y (V7 and later)	Y (V7 and later)	Y (V7 and later)
VMware Fault Tolerance supported [Y/N]	N	N	N
VMware Site Recover Manager (SRM) supported [Y/N]	N	N	N
VMware Tools supported [Y/N] (Note **)	Y (V7 and later)	Y (V7 and later)	Y (V7 and later)
VMware Distributed Resource Scheduler supported [Y/N]	Y (V7 and later)	Y (V7 and later)	Y (V7 and later)
VMware Data Recovery (VDR) supported [Y/N]	N (V7 and later)	N (V7 and later)	N (V7 and later)
VMXNET3 virtual network adapter supported [Y/N] Note: If supported please reference product specific installation/configuration documentation section for VMXNET3	N	N	N

NOTICE: * It is recommended to perform a Live Migration only in periods of low traffic, otherwise noticeable service interruption might occur.

NOTICE: ** Yes with the following exceptions: No gcc toolchain and kernel headers, not possible to build custom modules, see the Installation guide for more details.

NOTICE:

*** The values are valid from V10R1. For previous versions the valid values are:

Deployment	OS SBC 250	OS SBC 6000	OS SBC 20000
VM Memory [GB]	2 GB	2 GB	4 GB
VVM Memory Shares H = High N = Normal	N	N	N
VM Memory Reservation	2 GB	2 GB	4 GB
VM Memory Limit	2 GB	2 GB	4 GB

NOTICE:

****The default value is 2, but it is possible to configure up to 6 vNICs.

In some cases, it is necessary to add more NICs (network interfaces cards) after VM installation. In this case, it is possible that the order of the interfaces migh be incorrect. It is related to a known bug in SuSE knowledge base affecting SuSE VMs with 3 or more NICs. As a workaround, the following is suggested:

1) Use the console to verify the MAC address associated to eth interfaces using the command "ip addr".
2) In VMWare interface, select the VM and edit settings. Verify the MAC address used for NIC.
3) Associate the correct network adapter configured in VMWare host in NIC in accordance with MAC address verified in step 1.

NOTICE:

- OS SBC NW and Disk usage may vary based on call and registration rate.
- OS SBC figures in the table are based on no continuous tracing, default log level and configuration setting.
- VMotion/DRS during restart/patching/upgrade is currently not supported.

VMware Metrics

The following table and notes show the metrics for support of up to 20,000 OpenScape SBC SIP registered users.

Metric	250 (Note 1)	6000 (Note 1)	20000 (Note 1)

Maximum registered SIP Remote Users (Note 2), e.g., home workers (without Digest Authentication and without Throttling (Note 3))	250 (Note 4)	6,000 (Note 4)	20,000 (Note 4)
Maximum simultaneous SIP signaling calls / SBC sessions (half-calls) (Note 5)	150	1040	1760
Maximum simultaneous RTP media streams (full-calls) anchored through OpenScape SBC (Note 6,7,8)	75	510	850
Number of simultaneous SIP Service Providers (SSP)	10 (Note 9)	10 (Note 9)	10 (Note 9)
Avg.half-calls (Note 10) per sec.: • Off-net IP-trunk, incoming • Off-net IP-trunk, outgoing • On-net = ‘line to line’, originating • On-net = ‘line to line’, terminating	Total: < 1 <0.15 <0.15 <0.35 <0.35	Total: 3 0.5 0.5 1 1	Total: 4 0.75 0.75 1.25 1.25
Busy Hour Call Attempts - Full Calls (Note 10)	1500	23,400	39,600
Maximum peak half-calls (Note 10) per second (without Digest Authentication and without Throttling (Note 3) or TLS)	1	13	22
Registration refresh requests per second (randomized registration steady state condition)	<1	4	12
Steady state call completion rate	99.999%	99.999%	99.999%

The following notes provide details for the VMware Metrics:

NOTICE: Network interface switch speed is set to 1 Gigabit Ethernet.

NOTICE: For keysets, each keyset line appearance is counted as one registered user.

NOTICE: Throttling is a mechanism used to keep a NAT/firewall pinhole open for the subscriber's SIP signaling connection for a subscriber that is behind a farend NAT/firewall. In order to do this, REGISTER coming in from the subscribers are responded back with the small expiry interval (configurable, default 60secs) to force the subscribers to re-register causing the pin-hole in the NAT device to remain open.

NOTICE:

Add the following penalty (or penalties*) to get the actual registered SIP users limit. To get new numbers, apply penalty 1 and on the new numbers apply penalty 2.

a. Digest Authentication penalty: 25%

b. Throttling Penalty (60 seconds - reducing this value introduces more penalty): 60%

* To determine cumulative penalties apply penalty 1 and on the new number apply penalty 2.

** Throttling penalties are not applicable to hosted remote Branch users.

NOTICE: An SBC Session is defined as a SIP signaled call with an access-side signaling leg and a core-side signaling leg. A typical voice call between a local OpenScape Voice user and a Remote User registered via the SBC, or to a SIP Trunk connected via the SBC requires one SBC session. A typical video call requires two SBC sessions; one for the video connection and another for the audio connection. An additional 20% penalty on OpenScape SBC capacity should be added for a video connection versus an audio connection due to the extra SIP INFO messages that are exchanged during a video call.

NOTICE: Each RTP stream (full-call) anchored through the central OpenScape SBC consists of two half-calls travelling in opposite direction. For example, two half-calls are used when a remote user registered via the SBC is connected to another remote user registered via the SBC, or to a SIP Trunk connected via the SBC. A single half-call is used when a local subscriber registered directly with the OpenScape Voice server is connected to a remote user registered via the SBC, or to a SIP Trunk connected via the SBC.

NOTICE: Each RTP stream (full-call) anchored through the central OpenScape SBC consists of two half-calls travelling in opposite direction. For example, two half-calls are used when a remote user registered via the SBC is connected to another remote user registered via the SBC, or to a SIP Trunk connected via the SBC. A single half-call is used when a local subscriber registered directly with the OpenScape Voice server is connected to a remote user registered via the SBC, or to a SIP Trunk connected via the SBC.

NOTICE:

Note 7: The RTP packet performance (e.g., packet loss) is influenced by several factors:

a. Hardware BIOS settings relating to performance & power saving,

b. Hardware BIOS hyper-threading,

c. VM guest settings hyper-threaded core sharing,

d. VM guest memory (RAM),

e. VM guest OS NIC rx ring buffer size.

NOTICE: RTP packetization time/size. For better performance, choose BIOS performance over power-saving, disable HT, no HT core sharing. Multiple, active VM's and smaller vRAM allocations may decrease RTP packet loss.

NOTICE: Up to 10 SSP connections are supported. These connections can come from the same or different SSPs assuming the IP addresses on the SSP side are different. The SSP connection can point to the same or different IP addresses on the OpenScape SBC.

NOTICE: A "half call" is a call from either Access side (WAN) to core-side (LAN) or from core-side (LAN) to access-side (WAN). A "full call" consists of two half call legs. i.e. a call being initiated by the Access side (WAN) going to core-side (LAN) and then coming back to the Access side (WAN).

Overhead Requirements for Hosting OpenScape SBC

The following table lists the overhead requirements per physical server hosting OpenScape SBC.

Hardware	Description	Type
HD	VMware system disk overhead	17 GB
HD	Overhead for swap space for all unreserved VM memory	This value cannot be strictly defined because it is based on other VMs the customer may host on the physical server that are not configured to reserve all their (VM) memory
RAM	VMware system overhead	2.5 GB
CPU	VMware system overhead	See the vSphere Resource Management Guide

4.2.2 Checklist for Virtualization

This procedure assumes the steps 1-7 in the Virtual Machine Environment Setup have already been completed. Please review steps 1 through 7 before proceeding to install the "Virtual Machine". For installation of a "Virtual Appliance" (vApp) the procedure assumes the virtual environment is already operational.

Prerequistes:

- License activation codes have been secured.
- Configuration file is available (optional).
- Ethernet switches are installed.
- Servers are installed e.g., IBM x3550 M5.
- Create the VM using ESXi.
- Set the VM to boot off the ISO Image (virtual CD/DVD drive).
- Common Management Platform (CMP) is installed.
- The OpenScape SBC can be configured using CMP or Local GUI.

Virtual Machine Environment Setup:

1) Determine if Physical Server hardware is supported by VMware.
2) Determine if the local hard disk of this server will be the datastore or if a SAN will be connected.
3) If a SAN will be connected, determine if it is supported by VMware.
4) Have an operational USB Stick Setup Tool at hand in order to build the ISO Image.
5) Determine the Network Port to VMNIC mapping.
6) Determine what kind of installation configuration you will be conducting (Single or Redundant).
7) Determine network cabling based on the decisions made in steps 5 through 6.
8) Create the OpenScape SBC Software reference ISO image to the VM datastore. Instead of a USB, the OpenScape SBC ISO Image is used for the guest VMs.

> **NOTICE:** The ISO image must contain a valid image of the OpenScape SBC and IPs configured, created with the USB wizard tool.

9) Create the guest VMs according to the specifications or using vApps.
10) Install the OpenScape SBC ISO Image on the guest VMs created.

Virtual Appliance Environment Setup Using vApps

Virtual Appliance Setup - Overview

There are two ways a Virtual Appliance can be delivered:

- Ready to operate:

  The virtual appliance is fully operational when delivered. Usually, the OpenScape SBC appliance contains one or more appliances or applications e.g. OS voice, OpenScape SBC and other appliances. The virtual appliance is created using the vSphere Host client and vApps.

- On-site installation:

  The virtual appliance is installed by the customer or maintained by the customer using the vSphere Host client and vApps.

The main steps to create and install a virtual appliance is as follows:

1) Use the USB stick setup tool to create the ISO image with the software and node.cfg file for the virtual appliance.
2) Download the vApps template for the appliance.
3) Deploy the vApps.
4) Connect the USB stick ISO image to the Virtual Machine.
5) Boot using the USB stick ISO image.
6) The vApps gets configured with IP and other attributes from the USB stick ISO image.
7) Login to the Local GUI and install the system; then disconnect ISO and reboot.
8) Provision the OpenScape Session Border Controller using the CMP or Local GUI.

Upgrade of a Virtual Machine (VM)

To upgrade an existing VM install new software on the backup partition.

Migration from Native Hardware (HW) to Virtual Machine (VM)

To migrate from native HW to Virtualized OpenScape SBC deployment install the OpenScape SBC software on the virtual machine using the config files from the native HW deployment (modified by the USB Stick Tool to indicate the new deployment HW is "Virtual").The XML database may need to be adjusted prior to using the USB Stick.

4.2.2.1 How to Create an ISO Image

Proceed as follows to create an ISO image for virtual OpenScape SBC installation:

Prerequisites

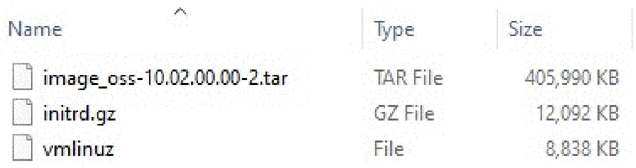
The USB stick setup tool and the software image files are available on a local PC.

The VMware vSphere client is available.

Step by Step

1) Extract the USB Stick Setup tool application from the zip file.

2) Copy the software image *.tar files into the ob folder. The folder will contain SW images for OpenScape Session Border Controller SW installation.



Name	Type	Size
image_oss-10.02.00.00-2.tar	TAR File	405,990 KB
initrd.gz	GZ File	12,092 KB
vmlinuz	File	8,838 KB

In this example, the base software file is *image_oss-01.00.01.5.tar* to be used for installing or upgrading.

3) Connect the USB stick to a USB port on the PC.

4) Proceed to the USB stick creation by running the usbsticksetup.exe application.

NOTICE: If doing a full installation using an existing DataBase (.xml), please make sure that the DB is exported from OpenScape Session Border Controller prior to start building the ISO Image. Via OpenScape SBC Local GUI, select the **Import/Export** configuration menu and export the xml file. The exported config file will be selected in the following step under installation method as “Already existent database file”.

The **USB Stick Setup** screen is displayed.

5) In the **USB Stick Setup** screen:

a) In the **Media Select** field, ensure that the **Virtual Machine ISO image** is selected.

b) Select **Generate node.cfg file** to create a new configuration file. Network interfaces configuration is required with this option.

NOTICE: If you select either the **Already existing database file or Already existing node.cfg file** option as the Installation Method the ISO image is created with data from the *.xml or *.cfg file you specify. With either option: the Host Name, IP Address, Subnet mask, and Default gateway (LAN only) fields are inactive (grayed out) and cannot be changed here. If you are using an *.xml or *.cfg as a template to install a new OpenScape Session Border Controller specific parameters will have to be specified or modified as necessary during the configuration process. The database file option can not be used for different hardware types.

c) Select the virtual hardware type from the **Hardware Type** list field.

d) In the **Host Name** field, enter a name for the system.

e) Set the interface type in the **Interface** list field to **LAN Interface**.

f) In the Network fields, specify the **IP Address, Subnet mask**, and **Default gateway** for the LAN/WAN Interfaces.

g) Click **OK**.

A warning message is displayed: "All partitions of the removable media will be deleted and a single FAT32 partition will be created."

6) Click **Yes** to continue.

   A progress bar is displayed.

7) When the **Save As** message appears, click **OK**.

   A **USB Stick setup complete** message is displayed to indicate the completion of the process.

8) Save the file with any name that matches the SBC being installed. Typically hostname and or IP and selects “Save As Type" **ISO Files (*.iso)** from the list field.

9) Click **Save** to complete the creation of the ISO image.

After the process is completed, the ISO Image is used to create the virtual SBC.

4.2.2.2 Creating a Virtual Machine on VMware

Proceed as follows to install the OpenScape SBC virtual machine on the server. This procedure is performed using the VMware vSphere Host client.

Prerequisites

The server hardware has been installed.

The ISO image has been prepared.

VMware and vSphere Host client is operational.

Common Management Platform (CMP) is installed or use Local GUI.

NOTICE:

The process to create a virtual machine may vary based on the third party vendor client application.

Step by Step

1) Copy the **ISO** file to the datastore using the VMware vSphere Host client.

2) Using the VMware vSphere Host client create a new virtual machine configuration for OpenScape SBC as described below:

a) Select **Create/Register VM**, the screen **New virtual machine** is open. In **Select creation type** choose the option **Create a new virtual machine** and click the **Next** button.

The **Select a name and guest OS** screen is displayed.

b) Enter the name of the OpenScape SBC virtual machine in the **Name** field. The name must be unique for each virtual machine and can contain up to 80 characters.

Choose the option to **Compatibility (EsXi 6.5 virtual machine or higher)**, **Guest OS family(Linux)** and **Guest OS version (Other 2.6x Linux(64 bit))**.

Click the **Next** button.

The **Select** storage screen is displayed.

c) Select the **datastore** (Name) from the datastore list display in which to store the OpenScape SBC virtual machine file and click the **Next** button.

The **Customize settings** screen is displayed.

d) Select the CPU, Memory and Hard Disk capacities in accordance with the desired Hardware Type:

Deployment	Virtual OSS-250	Virtual OSS-6000	Virtual OSS-20000
CPU	2	4	8
Memory (GB)	4	4	6
HD size (GB)	40	40	60

The number of processors in use depends on the number of licensed CPUs on the host and the number of processors supported by the guest OS.

By default, the parameter CPU Reservation is configured as *None* and CPU limit is configured as *Unlimited* if the virtual machine has been installed manually.

If the virtual machine has been installed using vApps, the specified values are reserved in accordance with the values shown in the table.

The same procedure applies to the amount of Memory.

When deploying vApps these values are set automatically (based on the 2.5 GHz core processor).

In OVF file in vApps, the CPU reservation is configured for Virtual OSS 250 (5000 MHz), Virtual OSS 6000 (10000 MHz) and Virtual OSS 20000 (20000 MHz).

Regardless if VM has been created manually or with vApps, these values need to be adjusted to fit the host processor capabilities. Other critical applications running at same host need to be taken into consideration as well.

The recommended settings for the reservation is the number of cores used by OSB/SBC multiplied by the core frequency of host processor.

Select the Hard Disk size for the virtual machine. The value should be set to e.g., Hard Disk = 60 GB.

Choose Thin or Thick provisioned option.

- **Thin:** This method helps you eliminate storage underutilization problems by allocating storage space in a flexible on-demand manner.
- **Thick:** Traditional method of storage provisioning. With thick provisioning, large amount of storage space is provided in anticipation of future storage needs. The space might remain unused causing underutilization of storage capacity.

e) Set the number of network interfaces based on the Hardware Type. Use the option **Add network adapter** to increase the number of NICs in virtual machine. In Network adapter uses **VMXNET3** option in **Adapter Type** field.

Connect at Power On checkboxes is activated for the NICs.

f) For **SCSI Controller** select the **LSI Logic Parallel** option.

g) Normally the virtual machine is created only with one **CD/DVD Drive 1**. Verify if the **controller location type** is using **SATA Controller 0 - SATA (0:0)**. The ISO file related to system software is added in this device.

> **NOTICE:**
>
> If the system is not detecting the CD/DVD, please change the **controller location type** from **SATA** to **IDE (IDE controller 0)** type.
>
> If ISO file related to database is used, add another CD/DVD device. Add using **Add other device**, **CD/DVD** drive option. **CD/DVD Drive 2** is using **SATA Controller 0 - SATA (0:1)**. Configure the ISO file repeating the procedure used to CD/DVD Drive 1.
>
> **Connect at Power On** checkboxes is activated for CD/DVD Drives.
>
> Click the **Next** button.
>
> The **Ready to complete** screen is displayed.

3) Prior to starting the task that will create the OpenScape SBC virtual machine, check the **virtual machine properties**. If it is necessary to correct some parameter, use the **Back** option to return to previous settings and change it.

4) Press **Finish** to complete the virtual machine creation.
The OpenScape SBC virtual machine is created.

5) Select the virtual machine and **Edit Settings**. In **CD/DVD Drive 1** change from **Host device** to **Datastore ISO file** option and select the ISO file in **CD/DVD Media**. Browse and Select the desired **ISO file** stored in datastore.

6) Power on the virtual OpenScape SBC. The virtual machine will boot from ISO image.

7) Follow the OpenScape SBC installation steps to complete the installation. The virtual OpenScape SBC virtual machine is created and installed.

NOTICE:

Once installation is complete, disconnect the CD/DVD Drive unchecking the **Connect at Power** checkbox on the **Virtual Machine Edit settings** window. Change also in **CD/DVD Media** from **Datastore ISO file** to **Host device**.

4.2.2.2.1 Creating a Virtual Machine on VMware (V11R2)

Starting from V11R2, the process for deploying OpenScape SBC on a virtual machine has been simplified. You can now deploy the OpenScape SBC virtual machine using the pre-configured OVA package, which automates much of the setup. This section outlines the updated procedure for performing a full installation of OpenScape SBC using the new deployment model.

Prerequisites

The server hardware has been installed.

The **OVA package** for OpenScape SBC has been obtained.

vSphere Host client is operational.

A **VMware ESXi** host is available for deployment.

The **Common Management Platform (CMP)** or **Local GUI** is installed for management, if needed.

NOTICE:

The process to create a virtual machine may vary based on the third party vendor client application.

Step by Step

1) Import the OVA Package:
   a) Open VMware vSphere Client and log in to your vSphere environment.
   b) Navigate to the Datastore where the OVA file is stored.
   c) Select Deploy OVF Template from the options.
   d) Browse to the location of the OpenScape SBC OVA file and select it.
   e) Click **Next**.
2) Open VMware vSphere Client and log in to your vSphere environment.
3) Click on the **Virtual Machines** button from the left-side menu.
4) Click **Create/Register VM**.

   The **New virtual machine** window pops up. By default, the **Select creation type** screen is dislayed.
5) Select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.
6) Click on the **Click to select files or drag/drop** area and navigate to the Datastore where the OVA file is stored.
7) Select the `.ova` file and click **Open**.

   The `.ova` file appears in the **New virtual machine** window.

8) Enter the name of the OpenScape SBC virtual machine.

> **NOTICE:** The name must be unique for each virtual machine and can contain up to 80 characters.

9) Click **Next**.

The **Select storage** screen is displayed.

10) Select the datastore in which to store the OpenScape SBC virtual machine file. By default, the first datastore from the displayed list is selected.

11) Click **Next**.

The **License agreements** screen displays the ULA license.

12) Click **I agree** to consent to the license, then click **Next**.

The **Deployment options** screen is displayed.

13) The **Network mappings** area displays the default network settings. Select which virtual networks to use for **MainLAN** and **MainWAN**.

14) Select any of the following options from the **Deployment type** drop-down menu:

- Small business, 250 users
- Mid-Enterprise, 6000 users
- Large, 20000 users

Upon selecting an option, the **Deployment Type** text field below the drop-down menu updates to display the required resources for the selected type.

15) By default, the **Disk Provisioning** is **Thin** and **Power on automatically** is enabled.

> **NOTICE:**
>
> - **Thin:** This method helps you eliminate storage underutilization problems by allocating storage space in a flexible on-demand manner.
> - **Thick:** Traditional method of storage provisioning. With thick provisioning, large amount of storage space is provided in anticipation of future storage needs. The space might remain unused causing underutilization of storage capacity.

16) Click **Next**.

The **Additional settings** screen is displayed.

17) Click on the **Application** drop-down menu to expand it.

a) Enter a hostname for the virtual machine in the **Hostname** text field.

> **NOTICE:** The hostname and the name of the virtual machine do not have to be the same. However, using the same name is recommended for easier identification.

18) Click on the **Networking** drop-down menu to expand it.

a) Enter the **LAN IP address**.

b) Enter the **LAN Netmask**.

c) Enter the **Default Gateway Address**.

19) Click **Next**.

The **Ready to complete** screen is displayed.

20) If needed, review the configurations you made.

21) Click **Finish** to complete the virtual machine creation.

The OpenScape SBC virtual machine is created. Note that this process may take a few seconds to complete.

The number of processors in use depends on the number of licensed CPUs on the host and the number of processors supported by the guest OS.

The CPU reservation is configured for Virtual OSB 250 (5000 MHz), Virtual OSB 1000 (10000 MHz) and Virtual OSB 6000 (20000 MHz).

These values are set automatically (based on the 2.5 GHz core processor), and need to be adjusted to fit the host processor capabilities. Other critical applications running at same host need to be taken into consideration as well.

The recommended settings for the reservation is the number of cores used by OSB multiplied by the core frequency of host processor.

22) Select the newly created OpenScape SBC virtual machine from the VMware vSphere Client.

23) Power on the virtual machine.

> **NOTICE:** This process will take a few seconds to complete.

The system will automatically boot using the **OVA package** and begin the installation process.

Once the virtual machine is powered on and running, the system will automatically detect the virtual resources and adjust to optimize performance.

If you need to adjust the settings (such as network configuration or hardware resources), you can modify them at this stage through the **vSphere Client**.

24) Connect to the OSB IP address

You are connected to the virtual OpenScape SBC virtual machine.

25) Optionallly, you can view the settings of the newly created virtual machine:

a) To view the network settings, navigate to **System** > **Network/Net services**.

b) To view the hostname, navigate to **System** > **Settings**.

26) The OVA image can also be used to upgrade the software. Simply select the ova files instead of the usual tar file (works on bare-metal servers as well):

a) Navigate to **Maintenance** > **Import/Export**.

The **Maintenance** window pops up.

b) Select the **Install/Upgrade** tab.

c) Click **Choose File** under the **Upgrade** area and browse to select it.

d) Click **Upgrade**.

4.2.3 Creating a Virtual Machine on Hyper-V

The .ovf templates provided in the vApps file are compatible only with VMware, so the Virtual Machine must be configured manually in Hyper-V.

Step by Step

1) Import the OVA Package:

a) Log in to your HyperV Manager.

b) Right-click the Hyper-V Manager and select **New** > **Virtual Machine**.

The **New Virtual Machine Wizard** window pops up.

2) Select **Specify Name and Location** from the left-side menu.

3) Enter the name of the virtual machine and select a location depending on the Hyper-V configuration.

4) Click **Next**.

The **Specify Generation** screen is displayed.

5) Select **Generation 1** and click **Next**.

The **Assign Memory** screen is displayed.

6) Configure the VM RAM memory according to the values indicated in the OpenScape Virtual Machine Resourcing and Configuration Guide.

NOTICE:

Do NOT check the **Use Dynamic Memory for this virtual machine** checkbox.

7) Click **Next**.

The **Configure Networking** screen is displayed.

8) In the VM creation wizard, only 1 NIC is added. If needed, you can add more after the VM is created.

9) Click **Next**.

The **Connect Virtual Hard Disk** screen is displayed.

10) Assign a virtual disk size according to the values indicated in the OpenScape Virtual Machine Resourcing and Configuration Guide:

a) Select the **Create a virtual hard disk** option.

b) Enter a Name.

c) Browse to select the location.

d) Enter the disk size (GB).

11) Click **Next**.

The **Installation options** screen is displayed.

12) Select the **Install an operating system later** option and click **Next**.

Once the new VM is created, go to the **Settings** tab to finish (or adjust) further settings.

4.2.3.1 Configuring SBC-Hyper-V settings and installation

As an administrator, you can configure OSB-Hyper-V settings.

Prerequisites

You have completed the Virtual Machine on Hyper-V configurations.

Step by Step

1) Under Settings, click **Add Hardware**.
2) Optionally, you can add additional NIC cards (or other hardware) by selecting the devices you want to add and clicking **OK**.
3) Go to the **BIOS** menu and select the order in which boot devices are checked to start the operating system.
4) Go to the **Processor** menu.
   a) Select the number of CPU threads accoridng to the OpenScape Virtual Machine Resourcing and Configuration Guide.
   b) Set **Virtual machine reserve (percentage)** to 100.
5) Optionally, under the **Network Adapter** menu, select the Virtual switch.

   NOTICE:

   Before the 1st start, the field is empty (00-00-00-00-00-00).

   Once you added all the NIC required, start and stop the machine again.

   This will assign the NICs MAC address.
6) Go to **Network Adapter** > **Advanced Features**.
   a) Under the MAC address area, select the **Static** option.
   b) Click **OK**.
7) Go to **Management** > **Integration Services**.
   a) Uncheck the **Time synchronization** checkbox.
   b) Click **OK**.
8) Go to **Management** > **Smart Paging File Location**.
   a) Browse to select where to store the **Smart Paging Files** for this virtual machine.
   b) Click **OK**.
9) Go to **Management** > **Automatic Stop Action**.
   a) Enable the **Shutdown the guest operating system** option.
   b) Click **OK**.

   Once the virtual machine is created, mount the OpenScape SBC iso file and configure the machine to boot from CD/DVD drive.
10) Go to **IDE Controller** > **DVD Drive**.
    a) Enable the **Image file** option.
    b) Browse to select the OpenScape SBC .iso file.
    c) Click **OK**.
11) Follow the OpenScape SBC installation steps to complete the installation.

    After the installation is finished, make sure you unmount the .iso file and change the boot order so the disk will be the first device.

4.2.4 Creating a Virtual Machine on Proxmox VE

By default, nested virtualization is enabled. However, it is recommended to verify that it is active.

To check, open a SSH connection to the Proxmox server.

Run the appropriate command based on your CPU type:

- For Intel CPUs: `cat /sys/module/kvm_intel/parameters/nested`

  If the output is Y, nested virtualization is enabled.

  If the output is N, nested virtualization is disabled.
- For AMD CPUs: `cat /sys/module/kvm_amd/parameters/nested`

  If the output is 1, nested virtualization is enabled.

  If the output is 0, nested virtualization is disabled.

If nested virtualization is disabled, follow these steps to enable it:

- For Intel CPUs:

  Edit the configuration file by running: `/etc/modprobe.d/kvm.conf:`
  ```
  echo "options kvm_intel nested=1" > /etc/modprobe.d/kvm.conf
  ```
- For AMD CPUs:

  Edit the configuration file by running: `/etc/modprobe.d/kvm.conf:`
  ```
  echo "options kvm_amd nested=1" > /etc/modprobe.d/kvm.conf
  ```

After making these changes, reboot the Proxmox host to ensure the settings take effect.

4.2.4.1 Creating a Virtual Mahine on Proxmox

The .ovf templates provided in the vApps file are compatible only with VMware, so the Virtual Machine must be configured manually in Proxmox.

Step by Step

1) From the Proxmox GUI (PVE), select **Create VM**.

The **Create: Virtual Machine** window is displayed.

2) Under the **General** tab:

a) Enter a Virtual Machine name in the **Name** field.

NOTICE: Some special characters (like underscore) are not allowed by Proxmox.

b) Check the **Advanced** checkbox to be able to see additional options.

c) Click **Next**.

NOTICE: **Node** and **VM ID** fields are assigned automatically, no changes are needed.

3) Go to the **OS** tab and select the **Do not use any media** option.

4) Go to the **System** tab and ensure that the **SeaBIOS** option is selected (default).

   Do not change this to a UEFI installation, since is not supported by OpenScape SBC VM.

5) Go to the **Disk** tab and select the required storage.

   if more options are available (depending on the Proxmox Cluster configuration), select the Disk size based on the values in the OpenScape Virtual Machine Resourcing and Configuration Guide.

   NOTICE: KVM hypervisors calculate the disk and memory size in GiB instead of GB.

6) Go to the **CPU** tab and select the number of CPUs accoridng to the values in OpenScape Virtual Machine Resourcing and Configuration Guide.

   a) Use 1 socket for all CPUs (eg. For 4 CPU, use 1 socket and 4 Cores instead of 4 sockets and 1 Core).

   b) From the **Type** dropdown menu, select **host**.

      The CPU type "host" should be used for optimal performance. However, only enable this if all CPUs in the cluster servers are identical to avoid potential issues during Virtual Machine migration between servers.

   c) Click **Next**.

7) Go to the **Memory** tab and configure the needed RAM Memory based on the information from the OpenScape Virtual Machine Resourcing and Configuration Guide.

   a) Disable the **Ballooning Device** checkbox so that the Memory is reserved and not shared by the OpenScape 4000 machine.

      NOTICE: KVM hypervisors calculate the disk and memory size in GiB instead of GB.

   b) Click **Next**.

8) Go to the **Network** tab and configure one NIC. Proxmox Virtual Machine creation wizard only allows adding 1 NIC.

   NOTICE:

   The Proxmox Virtual Machine creation wizard allows adding only one NIC. If additional network cards are needed, they can be added after the Virtual Machine is created, following the guidelines in the OpenScape Virtual Machine Resourcing and Configuration Guide.

Next steps

Once the Virtual Machine is created, you can configure the hardware settings in the Hardware menu, by performfing the following actions:

- Add multiple NIC cards.
- Mount/unmount the .iso image needed for the installation.

Additionally, you can change the boot order from the **Options** menu.

4.2.4.2 SBC Installation on Proxmox Hypervisor

Once the virtual machine (VM) is created, upload the OpenScape SBC iso file.

Prerequisites

You have created the virtual machine on Proxmox, as described in Creating a Virtual Mahine on Proxmox on page 135.

Step by Step

1) Log in to the Proxmox Web Interface.

2) Locate the Virtual Machine.

3) On the left-hand side, select the node where your Virtual Machine is located.

4) Under the VM list, click on the Virtual Machine that you want to mount the SUSE ISO to.

5) With your VM selected, click on the **Hardware** tab at the top of the VM's settings page.

6) Under Hardware, locate the **CD/DVD Drive** and select it.

> **NOTICE:** If a CD/DVD drive is not already listed, click **Add** > **CD/DVD Drive** to create one.

7) Click **Edit** at the top of the Hardware list.

The CD/DVD Drive settings window appears.

8) Select the ISO image you want to mount by clicking on the **ISO Image** drop-down list.

9) Browse through the available ISOs or upload the SUSE ISO to your Proxmox storage if it’s not already available.

10) To upload the ISO:

a) Go to the **Storage** tab on the Proxmox web interface.

b) Select the storage location (e.g., local, local-lvm, or another storage).

c) Under the **Content** section, click **Upload** and select the SUSE ISO file from your local machine.

d) Once the ISO is selected, click **OK** to confirm the changes.

11) Modify the Boot Order (if necessary):

a) Ensure that the CD/DVD Drive is listed before the hard drive in the boot order.

b) Go to the **Options** tab for your VM, find the **Boot Order** section, and click **Edit**.

c) In the boot order list, ensure the **CD/DVD Drive** is at the top. If not, use the **Move Up** button if needed.

d) Click **OK** to save the changes.

12) Once the ISO is mounted and the boot order is adjusted, go back to the **Summary** tab of the VM.

13) Click **Start** at the top of the page to power on the VM.

14) After the VM starts, click on **Console** in the menu bar at the top.

The Proxmox console will open, displaying the VM’s screen. You should see the SUSE boot or installation screen, depending on the ISO type.

15) Follow the OpenScape SBC installation steps to complete the installation.

Next steps

After the installation is finished, make sure you unmount the iso file and change the boot order so the disk will be the first device.

4.2.5 How to Display System Information

Perform the following steps to display system information for a Virtual OpenScape SBC. Display of system information for a virtual or physical SBC uses the same procedure.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC type is configured and in operation.

The OpenScape SBC must be created in the OpenScape Voice.

Step by Step

1) Navigate to `Maintenance tab` > `Inventory` > `Nodes`.
   The system presents the list of nodes with a current list of all known systems of all kinds.
2) Select a node of the OpenScape SBC type:
   a) Use the **Search for** and **in** fields to filter the list for OpenScape SBC systems.
   b) Click the name of an Open Scape SBC node.

   The system presents the **Dashboard** view of the selected node.
3) View the **System Info** field area. The following information is provided:
   - CPU Usage:

     Percentage of CPU processing power used.
   - Memory:

     Percentage of available memory used.
   - Disk Usage:

     Percentage of available disk space used.
   - Date and Time:
   - System Uptime:

     Time in days hours and minutes the system has been active from the last restart.
   - Hostname:

     Name given to the server/node for identification.
   - Operatig System:

     OpenScape based operating system e.g., openSUSE Leap 15.3.
   - Hardware type:

     Physical hardware type e.g., Lenovo x3550 and for virtual hardware type e.g. Virtual OSS 250. The **System Information** is displayed for the selected SBC.

4.3 Deployment of OpenScape Session Border Controller VirtualAppliance in the Form of a vApp

This chapter describes how to deploy the OpenScape Session Border Controlller virtual appliance in the form of a vApp. This procedure is performed using the ESXi 6.5 or higher. It can be managed by any web browser using the VMware Host Client, which is based on HTML5 technology. The process to create avirtual appliance may vary based on the third party vendor client application.

4.3.1 How to install the virtual machines using OpenScape SBC vApps

This chapter describes how to select the creation and storage type of the new virtual machine.

Prerequisites

The server hardware has been installed with respective VMWare esxi..

Download vApps from SWS and unzip the vApps files.

The ISO image has been prepared. Refer to How to Create an ISO Image on page 125 section in this document (page 114).

VMWare and vSphere Host client are operational.

Step by Step

1) Select the profile associated with the virtual appliance you want to create. The profiles are located where the vApp zip files were un-compressed. Otherwise select **Create / Register VM** > **Deploy a virtual machine from an OVF or OVA file** and click **Next**.
2) Enter the name of the OpenScape SBC virtual appliance in the Name field. The name must be unique for each vCenter Server VM folder and must contain up to 80 characters.
3) Select one of the following profiles:
   a) **OSS-250**
   b) **OSS-6000**
   c) **OSS-20000**
4) Select the **.ovf** and **.vmdk** files and click **Next**.
5) Select the destination storage from the datastore list display to store the OpenScape SBC virtual appliance files on the **Storage** screen and click **Next**.
6) Configure Network mappings. Set the appropriate LAN and WAN interfaces with the ESXI Server.
7) Select one of the available Disk Provisiong options:
   a) **Thin**: This method helps you eliminate storage underutilization problems by allocating storage space in a flexible on-demand manner.
   b) **Thick**: Traditional method of storage provisioning. With thick provisioning, large amount of storage space is provided in anticipation of future storage

needs. The space might remain unused causing underutilization of storage capacity.

NOTICE: Using thick eager-zeroed virtual disk reduces delays the first time that a block is written to the disk and ensures that all space is allocated and initialized at creation time.

8) Enabling the **Power on automatically** option, the virtual machine is started automatically after finishing the installation process. Click **Next**.

9) Verify the deployment settings displayed in the work area on the **Ready to Complete** screen and click **Finish**.
The deployment will start and run to completion. When the process is completed, the virtual OpenScape SBC appliance will be ready to power on.

NOTICE:

When deploying vApps these values are set automatically (based on the 2.5 GHz core processor). In OVF file in vApps, the CPU reservation is configured for Virtual OSS 250 (5000 MHz), Virtual OSS 6000 (10000 MHz) and Virtual OSS 20000 (20000 MHz).

Regardless if VM has been created manually or with vApps, these values need to be adjusted to fit the host processor capabilities. Other critical applications running at same host need to be taken into consideration as well.

The recommended settings for the reservation is the number of cores used by OSB/SBC multiplied by the core frequency of host processor.

If the resources are not available in used VMWare Host server or due to the processor type, the following messages can be received in virtual machine power on:

“Failed - The amount of CPU resource available in the parent resource pool is insufficient for the operation."

Errors

- Module 'MonitorLoop' power on failed.
- Group vm.8998268: Cannot admit virtual machine: CPU admission check failed.

  Invalid reservation 20000 mhz.
- Group host/user: Invalid CPU allocation requested for virtual machine vmm0:SBCConfigDemo. (min: 20000 mhz, max: 20000, minLimit: -1, shares: -3)
- Could not power on virtual machine: Admission check failed for cpu resource. See the VMware ESX Resource

Management Guide for information on resource management settings.

- Failed to power on VM.
- Failed to start the virtual machine.

"Failed - Module 'MonitorLoop' power on failed."

Errors

- Module 'MonitorLoop' power on failed.
- Group host/user: Invalid CPU allocation requested for virtual machine vmm0:SBCConfigDemo. (min: 20000 mhz, max: 20000, minLimit: -1, shares: -3)
- Could not power on virtual machine: CPU min outside valid range.
- Failed to power on VM.
- Failed to start the virtual machine.

In this case, it is necessary to set the parameter **Reservation** to a value that fits the host processor capabilities (considering also other applications) and parameter Limit=Unlimited.

To avoid this risk, close monitoring of the SBC CPU usage is recommended. An alarm is raised in case there is a high CPU usage.

4.3.2 How to select the OpenScape SBC software to installation in virtual machine

This chapter describes how to select the software to complete the installation of OpenScape SBC virtual machine.

Step by Step

1) Click the **Edit settings** for Virtual Machine.

2) Verify the **CD/DVD Drive 1** and **CD/DVD Drive 2**. Please select the **CD/DVD Drive** that is associated with **IDE Controller 0(IDE 0)**.

NOTICE:

The other CD/DVD Drive is associated to IDE Controller 1(IDE 1), that is used to connect the ISO related to xml database. If it is not used, this CD/DVD Drive associated to IDE Controller 1 can be removed.

3) Click on the **Connect at power on** checkbox in the **Device Status** work area.

4) Select **Datastore ISO File** in the **Device type** work area. For more information see How to Create an ISO Image on page 125.

5) Browse and select the Datastore ISO File associated with the OpenScape SBC, in the **Device type** work area.

6) Save the Virtual Machine configuration.

> **NOTICE:**
>
> Repeat the same procedure to connect SBC Configuration ISO file in CD/DVD Drive, if the file is available.

> **NOTICE:**
>
> If specific MAC address is required, then configure the MAC address before powering on the virtual appliance.
>
> Refer to How to set the MAC address of vApp (optional) on page 142 on page 117.

4.3.3 How to set the MAC address of vApp (optional)

This chapter describes how to set the MAC Address of the OpenScape SBC virtual appliance. If the MAC address of the virtual appliance is not set manually, the ESXI server will create a random MAC address.

Step by Step

1) Click the **Edit Settings** for Virtual Machine.
2) Select **Network Adapter 1** in the **Hardware** work area.
3) Check the **Connect at power on** checkbox in the **Device Status** work area.
4) Enter the **MAC address** in the **MAC Address field**.
5) Select **Manual** in the **MAC Address** work area and click **OK**.

   The virtual OpenScape SBC appliance is ready to power on.

4.3.4 How to complete the installation related to virtual OpenScape SBC

This chapter describes how to install the OpenScape Session Border Control virtual appliance.

Step by Step

1) Open a browser and enter the OpenScape SBC Function LAN IP address (defined previously with the OpenScape SBC USB Stick setup tool) via https:// in the address field.
   The OpenScape Border Control Function Management Portal login screen is displayed.
2) Log in to the OpenScape Border Control Function Management Portal using the following credentials:
   - username: **administrator**
   - password: **Asd123!.**
3) Click **OK** on the message **You are booting from USB stick/CDROM**.

   The **OpenScape SBC** tab is displayed.

4) Select **Maintenance** > **Install/Upgrade** to open the dialog window and click **Install**.

> **NOTICE:** All previous data in the system will be lost. If an USB stick or ISO image has been created with a Config/DB file then that will be applied during installation.

5) When prompted to confirm that you want to perform a full installation, click **OK**.
The installation process begins. Average installation time of an OpenScape SBC system is around 10 minutes. A progress bar will show the total installation progress.
6) When prompted with the message **System installed press OK to reboot the system now**, click **OK**.
7) Another prompt with the message **Please detach the ISO from your virtual machine CD/DVD drive before continue** is displayed. Refer to How to detach the ISO Files from the CD/DVD drives in Hypervisors on page 143 to configure detachment of ISO Files from the CD/DVD drive.
8) Click **OK** in response to the prompt **Please detach the ISO from your virtual machine CD/DVD drive** before continuing to reboot the OpenScape SBC.

> **IMPORTANT:** From V10, the open-vm-tools is installed in full install and the flag Enable Open VM Tools should be checked in System / Settings. If checked, this field enables the Open Virtual Machine Tools (open-vm-tools).

4.3.5 How to detach the ISO Files from the CD/DVD drives in Hypervisors

4.3.5.1 Detach ISO files in VMware

This chapter describes how to detach the ISO files from the CD/DVD drives in the Virtual Machine Settings, using the VMware Host Client via the web browser.

Step by Step

1) Select **CD/DVD Drive 2** and uncheck the **Connected at power on** option.
2) Change the **Datastore ISO File** to **Host device** option.
3) Select **CD/DVD Drive 1** and uncheck the **Connected at power on** option.
4) Change the **Datastore ISO File** to **Host device** option.
5) Click **OK** to save the Virtual Machine settings.

4.3.5.1.1 Detach ISO files in Hyper-V

Step by Step

1) Open Hyper-V Manager:

   Press `Win + X` on your keyboard and select **Hyper-V Manager** from the menu,

   or

   search for Hyper-V Manager in the **Start** menu.

   The **Hyper-V Manager** window opens.

2) Optionally, right-click on the VM in the list and select **Turn Off** or **Shut Down** to power it off.

   NOTICE:

   It is recommended to power off the VM before removing the ISO.

   While you can detach the ISO while the VM is running, it is safer to do so when powered off.

3) Right-click on the selected VM and select **Settings**.

   The VM's settings window opens.

4) In the left panel, locate the **IDE Controller** or **SCSI Controller**, depending on where the virtual CD/DVD drive is attached.
5) Under the controller, select the DVD Drive (e.g., DVD Drive 1).
6) To detach the ISO from the VM, click **Remove** under the Media section.

   NOTICE: It may display something like: `Image file: [ISO file path]).`

7) Click **OK** to save and apply the changes.
8) Optionally, if the VM was powered off, right-click the VM and select **Start** to power it back on.

4.3.5.1.2 Detach ISO files in Proxmox

Step by Step

1) Open your web browser and navigate to https://<your-proxmox-ip>:8006.
2) Enter your username and password to log into the Proxmox dashboard.
3) In the left panel, locate and select the VM that has the attached ISO.

   The VM details page opens.

4) Go to the **Hardware** tab at the top of the VM's page.
5) Locate and select the **CD/DVD Drive** entry, where the ISO image is attached.

   A menu with the **CD/DVD Drive** options appears.

6) To detach the ISO from the VM, click **Remove**. If prompted, confirm the action.

   Once removed, the CD/DVD drive in the Hardware tab no longer has an attached ISO file.

7) Click **OK** to save and apply the changes.

8) Optionally, if the VM was powered off, right-click the VM and select **Start** to power it back on.

5 Serviceability Features

OpenScape Session Border Controller maintenance and service tasks are performed via the OpenScape SBC Assistant, the OpenScape SBC Management Portal (local tool) and the OpenScape Voice Assistant CMP. The features listed below are documented in the OpenScape SBC Online Help (located in the OpenScape SBC Assistant).

OpenScape SBC Local Management Tool Versus Assistant

For a new installation and complete setup of an OpenScape Session Border Controller the OpenScape SBC Management Portal (local tool) provides all relevant configuration and service functions. When the LAN connection to the OpenScape Voice system is up, the OpenScape SBC Assistant may be used to maintain and configure the system as well.

Software Management and Monitoring

The following tasks can be performed:

- Restarting the system to the current configuration
- Restoring the system to the backup configuration
- Import/export configuration files
- Software activation
- Debugging the system
- Continuous tracing
- On demand tracing

Statistics

Statistics comprise current quantities of specific values of the SIP server or of an OpenScape Session Border Controller.

The following Information is displayed:

- SIP server: Active dialogs:

  The number of SIP dialogs currently active.
- SIP server: Requests In:

  The number of SIP requests received since the SIP server is in operation.
- SIP server: Requests Out:

  The number of SIP requests sent since the SIP server is in operation.
- SIP server: Responses In:

  The number of SIP responses received since the SIP server is in operation.
- SIP server: Responses Out:

  The number of SIP responses sent since the SIP server is in operation.

System Info

A list of registered subscribers can be displayed.

Dashboard

The Dashboard view of an OpenScape Session Border Controller can be displayed via the Common Management Platform (CMP). It provides a variety of performance and system information such as Alarm summary, system information and status of applications and actions. Several sub-windows provide advanced information.The dashboard view suits for the administrator as well as for the service technician to get a quick and global overview of the selected OpenScape Session Border Controller.

Alarms

The OpenScape SBC Assistant provides a table displaying all types of alarms and the respective parameters. For each type it is possible to edit the alarm parameters individually.

NOTICE: Please see the *OpenScape SBC Administration, Administrator Documentation*, for more information or use the OpenScape SBC Assistant online help.

5.1 How to Display OpenScape SBC using the Dashboard via CMP

Aggregated information and data for an OpenScape Session Border Controller (SBC) can be displayed in the "Dashboard View" via the Common Management Platform.

Prerequisites

Adequate administrative permissions.

At least one OpenScape Session Border Controller is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) In the Common Management Platform (CMP), under **Maintenance**, select the **Inventory** button, and select **Nodes** in the Navigation Tree.

The system presents the list of nodes with a list of all known systems of all kinds.

2) Select a OpenScape Session Border Controller node:

a) Use the **Search for** and **in** fields to filter the list for OpenScape SBC/ Branch systems.

b) Click the name of an OpenScape SBC node in the list.

The system presents the **Dashboard** view of the selected node.

5.2 Backup and Restore Procedures

This chapter describes several maintenance tasks.

Overview

The Import/Export menu option is used for the following:

- Backup a configuration file.
- Restore a configuration file.

- Change the system configuration by loading a different configuration file.

5.2.1 How to Load and Apply Configuration Files

Proceed as follows to change the configuration of an OpenScape Session Border Controller (SBC) the system using a new configuration file where all configuration settings are stored.

Prerequisites

Adequate administrative permissions.

At least one OpenScape Session Border Controller is configured and in operation.

The connection to the OpenScape Voice system is up.

NOTICE: Configuration done from CLI (ex. /etc/hosts, Manual DNS config, etc) will have to be backed up manually as it is not part of the XML.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under Administration.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list. Action Menu buttons are set active in the Work Area with the following options: **Manage**, **Local Password...**, **Refresh Selected**, **Edit...**, **Delete**. Selecting the **Manage** button updates the **Select OpenScape SBC** field, in the Navigation Tree, with the selected SBC and displays information and data in the Work Area for that SBC.
- Choose a SBC from the **Select OpenScape SBC** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- Enter filter search criteria to filter the list of SBC and branch offices.

  Filtering is possible on the following criteria from the **in** field: **OpenScape SBC** (name), **Business Group, IP Address, Version, Status, Mode.**

  > **NOTICE:** Wild cards are supported (* for 0 or more characters, "?" for single characters).

5) Navigate to **Configuration > System**.

The **System** window appears with the **General** tab selected by default.

6) Select the **Import/Export** tab.

The **File in use** field displays the name of the configuration file currently in use.

> **NOTICE:** The config_default.xml file contains the original basic xml including IP configuration.

7) To select a new configuration file use one of the following options:

- Select the configuration file in the **Use a new configuration file** field.
- Click the **Import** button and select a configuration file to be transferred to the system.

8) Click the **Load** button.

The system reads and stores the xml config file settings temporarily.

9) Click the **Close** button to close the **Import/Export** window.

10) Click the **Apply Changes** button in the main window to confirm the changes and start the action.

The configuration settings of the selected configuration xml (Extensible Markup Language) file is applied to the system. After Changes are done, the loaded config file will increment by 1.

Example

IBM3250IP70_config_47.xml will be replaced by IBM3250IP70_config_48.xml

5.2.2 How to Import or Restore a Configuration File

Proceed as follows to import a new configuration file where all configuration settings are stored.

Prerequisites

Adequate administrative permissions.

At least one OpenScape Session Border Controller is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape Office list** in the Navigation Tree under Administration.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list. Action Menu buttons are set active in the Work Area with the following options: **Manage**, **Local Password...**, **Refresh Selected**, **Edit...**, **Delete**. Selecting the **Manage** button updates the **OpenScape SBC** field, in the Navigation Tree, with the selected SBC and displays information and data in the Work Area for that SBC.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- Enter filter search criteria to filter the list of SBC.

  Filtering is possible on the following criteria from the **in** field: **OpenScape SBC** (name), **Business Group, IP Address, Version, Status, Mode.**

> **NOTICE:** Wild cards are supported (* for 0 or more characters, "?" for single characters).

5) Navigate to **Configuration > System**.

The **System** window appears with the **General** tab selected by default.

6) Select the **Import/Export** tab.

The **File in use** field displays the name of the configuration file currently in use.

7) Click the **Import** button.

The **Import** window appears.

8) Click the **Browse...** button to select the file name and path of the configuration file to be transferred to the system.

9) Click the **OK** button.

The **Import** window closes and selected configuration xml (Extensible Markup Language) is temporarily applied to the system. The **Apply Changes** button in the main menu becomes enabled and navigation in any of the configuration menu screens will indicate the temporarily imported configuration.

10) Click the **Apply Changes** button to set this configuration to the OpenScape SBC appliance.

After **Apply Changes** has been clicked, the loaded config file will be incremented by 1.

Example

<Host_name>-oss-config_47_20110521T113058.xml will be replaced by <Host_name>-oss-config_48_20110621T113124.xml

Parameters:

- <Host_name>: This is automatically generated in the file name.
- Version: 47
- Date: 2011 05 21 (year, month, day)
- Time: 11 30 58 (hour, minutes, seconds)

5.2.3 How to Export a Configuration File for Backup

Proceed as follows to export a configuration file where all configuration settings are stored.

Prerequisites

Adequate administrative permissions.

At least one OpenScape Session Border Controller is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under Administration.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC or branch office in the list. Action Menu buttons are set active in the Work Area with the following options: **Manage**, **Local Password...**, **Refresh Selected**, **Edit...**, **Delete**. Selecting the **Manage** button updates the **OpenScape SBC** field, in the Navigation Tree, with the selected SBC and displays information and data in the Work Area for that SBC.
- Choose an SBC from the **OpenScape SBC** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- Enter filter search criteria to filter the list of SBC.

  Filtering is possible on the following criteria from the **in** field: **OpenScape SBC** (name), **Business Group, IP Address, Version, Status, Mode.**

  > **NOTICE:** Wild cards are supported (* for 0 or more characters, "?" for single characters).

5) Navigate to **Configuration > System**.

The **System** window appears with the **General** tab selected by default.

6) Select the **Import/Export** tab.

The **File in use** field displays the name of the configuration file currently in use.

7) Select a configuration file in the **Select a configuration file to export** field.

Using the Export All feature; it is possible to generate a tar file which includes the 10 latest xml configuration files for export.

8) Click the **Export** button.

The **file Download** dialog opens.

9) Use one of the following options:

- Click the **Open** button to open and display the configuration file in the system´s xml (Extensible Markup Language) file viewer application.
- Click the **Save** button and specify the location of the configuration file to be exported. Then click the **Save** button in the **Save As** dialog.
- Click the **Cancel** button to abort the action and return to the **Export/ Import** window.

10) Click the **Close** button to close the **Import/Export** window.

The action is completed.

5.3 Users and Passwords

Passwords can be changed or reset to default depending on the user identity, the rights and the administration tool. Additionally, starting in V8 the SBC has the capability for centralized authentication of users and passwords via a pair of RADIUS servers.

Types of Users on the OpenScape SBC Assistant

The following users are available for login and can be configured in the **System** window:

User	Default Password
administrator	Asd123!.
root	T@R63dis
service	BF0bpt@x
guest	1clENtk=

User	Default Password
assistant	2GwN!gb4
redundancy	Asd!.123

IMPORTANT: It is strongly recommended that the default passwords be changed to different (secret) passwords during system installation.

NOTICE: Other users not applicable to OpenScape SBC i.e., ACD, cdr.

User rights for password change

The capability to reset passwords is base on the Management Interface the User is logged onto.

Management Interface	User	Rights to Change Password for
CMP (Assistant)	assistant	guest, assistant, administrator, service
Local GUI	administrator and service	guest, assistant, administrator, service, redundancy
	root	guest, assistant, administrator, service, root, redundancy
	guest	guest
CLI (ssh)	root (via sudo command)	guest, assistant, administrator, service, root
	service (via sudo)	guest, assistant, administrator, service, root

Default users rights/groups for OpenScape SBC / OpenScape Branch

Default user rights and groups are preset for each type of user.

User	Assistant	Local GUI	ssh/sftp	Groups
administrator	No access	Read and Write	ssh (Read only)	user, sshlogin
assistant	Read and Write	No access	sftp only	assistant, sshlogin
guest	No access	Read only	No access	user
root	No access	Read and Write	No access (Root privileges via ssh can be obtained by using sudo)	root
service	No access	No Access	ssh/sftp/scp (Read and Write)	sshlogin

User	Assistant	Local GUI	ssh/sftp	Groups
redundancy	No access	No access	ssh/sftp (Read and Write)	sshlogin

5.3.1 How to Change or Reset the Password

Proceed as follows to change or reset the login password for the access to the OpenScape Session Border Controller (SBC) system.

Prerequisites

Adequate administrative permissions.

At least one OpenScape Session Border Controller is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under Administration.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list. Action Menu buttons are set active in the Work Area with the following options: **Manage**, **Local Password...**, **Refresh Selected**, **Edit...**, **Delete**. Selecting the **Manage** button updates the **OpenScape SBC list** field, in the Navigation Tree, with the selected SBC and displays information and data in the Work Area for that SBC.
- Choose a SBC or branch office from the **OpenScape SBC** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- Enter filter search criteria to filter the list of SBC and branch offices.

  Filtering is possible on the following criteria from the **in** field: **OpenScape SBC** (name), **Business Group, IP Address, Version, Status, Mode.**

> **NOTICE:** Wild cards are supported (* for 0 or more characters, "?" for single characters).

5) Navigate to **Configuration > System**.

The **System** window appears with the **General** tab selected by default.

6) Select the **Password** tab.

7) To reset a password, proceed as follows:

   a) Select the user for whom the password shall be reset in the **Select user** selection list. Possible users: administrator, service, guest, assistant.

   b) Click the **Reset** button.

   The password will be set to default for the selected user.

> **NOTICE:** The users and their default passwords are referenced in chapter 5.3 Users and Passwords.

8) To change a password, proceed as follows:

   a) Select the user for whom the password shall be changed in the **Select user** selection list. Possible users: administrator, service, guest, assistant.

   b) Enter the old password in the **Old Password** field.

   c) Enter the new password of the OpenScape Session Border Controller in the **New Password** field. The password must be 8...36 characters.

   d) Enter the new password of the OpenScape Session Border Controller again in the **Confirm Password** field.

   e) Click the **Change** button.

   The password will be changed and a confirmation message is displayed.

9) Click the **OK** button to store the changes temporarily in the administrator´s login session.

   The **System** dialog disappears.

10) Click the **Apply changes** button in the main window.

The password is changed or set to default in the OpenScape Session Border Controller.

5.3.2 How to Enable RADIUS User Authentication

Proceed as follows to enable an OpenScape Session Border Controller (SBC) system for user authentication via a central pair of RADIUS servers. This eliminates the need to manage individual accounts on each SBC for networks with many SBCs.

Prerequisites

Adequate administrative permissions.

The OpenScape Session Border Controller is configured and in operation.

The RADIUS servers are configured and in operation.

> **IMPORTANT:** A Web or CLI user who is defined on the RADIUS server does not need to be defined on the OS SBC. When a user who is not defined on the OS SBC logs in via RADIUS, that user will be granted the privileges of the default ‘service’ user. This will then allow the user logging in to perform the type of functions that the service user can perform. If a

user attempts to log in to the Web or CLI application using a username that is only defined on the RADIUS servers, and the RADIUS servers are down, then login will fail. The user will need to attempt to login locally using one of the default usernames.

Step by Step

1) Login to the SBC local management portal via local administrative user and password.

2) Navigate to **Security > RADIUS**.

The **RADIUS** window appears.

3) Set the **Enable RADIUS** checkbox.

4) Enter the following information associated with the two RADIUS servers:

a) **Address** - the IP Address of server.
b) **Port** - the IP Port used by RADIUS server (normally 1812).
c) **Secret** - the security message digest used by the RADIUS server (must be 16 characters).
d) **Timeout** - for logins via the RADIUS server.

5) Set the **Enable RADIUS Authentication** checkboxes for the management interfaces as required by the specific customer deployment.

a) **CLI**
b) **SSH**
c) **WEB**

6) Set the **Enable RADIUS Accounting** checkboxes for the management interfaces as required by the specific customer deployment. This capability is sometimes used for statistical purposes.

a) **CLI**
b) **SSH**
c) **WEB**

7) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **System** dialog disappears.

8) Click the **Apply changes** button in the main window.
The user authentications will now be performed by the RADIUS servers.

5.4 Remote Administration for Standalone Servers

Administration for a standalone OpenScape SBC without a Common Management Platform (CMP) is performed by the OpenScape SBC Management Portal (Local GUI). Since the OpenScape SBC is normally protected by a firewall, a tunnel must be created to allow administrative access. This tunneling capability is supported for V7 and later releases of the OpenScape SBC.

General Concept

To allow access to the Local GUI, the OpenScape SBC device must support the Smart Services Delivery Platform (SSDP). A SSDP plug-in resides in the server software and can be enabled, disabled and be monitored via the Local GUI. SSDP provides a tunnel to the Local GUI from the OpenScape SBC device to the service technician’s workplace. The service technician work in a Secure Infrastructure for Remote Access (SIRA) environment.

The SSDP plug-in in conjunction with the SSDP Enterprise server enables the remote service technician to use functions of the OpenScape SBC Local GUI including:

- OpenScape Branch software installation
- File transfer
- Retrieval of last restart date and time for the device.
- Display of software version, Product name (OS SBC), and HW type.

5.4.1 How to Enable Smart Service Delivery Platform (SSDP) for Stand Alone Remote Administration

Proceed as follows to enable the Smart Service Delivery Platform plug-in for remote administration access to a standalone OpenScape SBC device. This feature is supported in OpenScape SBC for V7 and later releases.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

Step by Step

1) Open the local OpenScape SBC Management Portal (Local GUI) for the OpenScape SBC.

2) Select **System > Settings** within the Navigation Bar in Local GUI.

3) Checkmark the **SSDP Enable** checkbox in the Administration Work Area and click the **OK** button.

4) Click the **Apply Changes** button in the main window to confirm the changes and start the action.

The SSDP plug-in system is enabled and remote access to the Local Administration GUI is available.

NOTICE: The SSDP plug-in only needs to be enabled once in the Local Administration GUI. When enabled the SSDP plug-in will automatically run even after the OpenScape SBC restarts.

NOTICE: : It may be necessary to configure the SSDP plug-in with an HTTP proxy server via the Axeda Deployment Utility so the SSDP plug-in can contact the SSDP Enterprise Server.

5.4.2 How to Display Smart Service Delivery Platform (SSDP) Status

Proceed as follows to display the Smart Service Delivery Platform status used plug-in for remote administration access to a standalone OpenScape SBC device. This feature is supported in OpenScape SBC for V7 and later releases.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

Step by Step

1) Open the local OpenScape SBC Management Portal for the OpenScape SBC.

2) Select **Dashboard** within the Navigation Bar in Local GUI.

3) Click the **Services status Show** button in the System Status Work Area.

The Services status window appears with the current status of available services. The SSDP status is displayed.

6 OpenScape Branch and OpenScape SBC Licensing Files

For OpenScape Branch, OpenScape Session Border Controller and associated applications different license types and license files are available.

License File Generation

A License file can be generated in one of two ways: Generated for Centralized Licensing Management via Common Management Platform (CMP) or generated for Stand Alone Mode License Management via the local GUI administration.

- **Centralized License Management**

  The license file is generated using the MAC ID of the Common Management Platform.

  This license file can be offline activated/applied via the CMP. Optionally, a License Authorization Code (LAC) can be used to online activate/apply a license file via the CMP.
- **Stand Alone Mode License Management**

  Stand Alone Mode management is used when the OpenScape Branch or OpenScape SBC is deployed at a customer who does not have a Common Management Platform (CMP) with OpenScape SBC Assistant / OpenScape Branch Assistant or the CMP is not upgraded to a version that supports OpenScape Branch licensing.

  The stand alone license file must have been previously generated and supplied to the customer, using the MAC ID of the OpenScape Branch or SBC. These customers use the OpenScape Branch or OpenScape SBC local GUI to manage the OpenScape Branch or OpenScape SBC

.

Licensing Files

The following types of license files are supported:

- **Regular License Files** (RLF) contain licenses purchased by the customer. Regular Licenses have no expiration date.

  OpenScape Branch License file:

  The following types of files are contained in the OpenScape Branch License file:

  – OpenScape Branch Base Licenses (maximum allowed 3,000)
  – OpenScape Branch Registered Lines licenses (maximum allowed 100,000)
  – Auto Attendant Licenses (maximum allowed 3,000)
  – Backup ACD Licenses (maximum allowed 3,000)

  OpenScape SBC License File:

  The following types of files are contained in the OpenScape SBC License file:

  – Centralized SBC Base Licenses (maximum allowed 100)
  – OpenScape SBC Session Licenses (Maximum allowed 160K for Branches and 40K for OpenScape SBC)

- **Software Subscription License File** is a Regular License file that expires on Jan 31st and will contain the maximum values possible for each OpenScape Branch and OpenScape SBC license type.

  OpenScape Branch File:

  – 3,000 OpenScape Branch Base Licenses
  – 100,000 OpenScape Branch Registered Lines licenses
  – 3,000 Auto Attendant Licenses
  – 3,000 Backup ACD Feature Licenses

  OpenScape SBC File:

  – 100 Centralized SBC Base Licenses
  – 200,000 OpenScape SBC Session Licenses (160K for Branches and 40K for OpenScape SBC)
- **Evaluation License File** is a Regular License File with an expiration time of 180 days. The Evaluation License File shall contain the following licenses:

  OpenScape Branch File:

  – 1 OpenScape Branch Base License (if evaluating OSB)
  – 1 Auto Attendant Feature License (if evaluating OSB)
  – 1 Backup ACD Feature License (if evaluating OSB)
  – 50 OpenScape Branch Registered Lines licenses (if evaluating OSB)

  OpenScape SBC File:

  – 1 OpenScape SBC Evaluation License (if evaluating SBC)
  – 100 OpenScape SBC Session Licenses (if evaluating OSB or SBC)

Redundancy

A license quantity is needed for the Redundant feature in V11 in the following cases:

- When the system is redundant with V10 Licenses and then is upgraded to V11 Licenses.
- When the Redundancy feature is initially activated in V11, either in a fresh or an upgraded system.

Only one license is needed per each redundant system since the active node populates its licensing to the backup node. No additional licenses are required for the backup node.

6.1 OpenScape Regular License File (SBC and Branch)

OpenScape SBC Assistant and OpenScape Branch Assistant support Regular License files. The Regular license is a customer purchased license that does not expire.

License Functionality

- The OpenScape Branch Regular license file provides the license types and quantities necessary for a customer to use OpenScape Branch functionality, including Branch base functions, Branch Users, Auto Attendant feature, Backup ACD feature without expiration
- The OpenScape Session Border Controller (SBC) Regular license file provides the license types and quantities necessary for a customer to use

OpenScape SBC functionality, SBC base functions and SBC sessions without expiration.

License Monitoring

- OpenScape SBC Assistant / OpenScape Branch Assistant is informed by the License Management service that a new RLF license file has been applied including the total number of OpenScape SBC / OpenScape Branch licenses for each license type and the expiration date of the license file. OpenScape SBC Assistant / OpenScape Branch Assistant will then check to ensure the number of licenses in the RLF is enough to accommodate the number of configured licenses for all devices. If not, OpenScape SBC Assistant / OpenScape Branch Assistant provides a popup to inform the craft the RLF license file does not have enough licenses. In this situation OpenScape SBC Assistant / OpenScape Branch Assistant will also return license values of zero to all devices requesting a license update until a license file with enough licenses is applied to the system.
- If the RLF license file has enough licenses to accommodate all the devices, OpenScape SBC Assistant / OpenScape Branch Assistant will check-out the licenses for each device.
- The OpenScape SBC / OpenScape Branch will display a popup at least once a day whenever any license file is within 60 days of expiration and whenever configuration is not possible due to the inability to check-out a license. The popup will be shown when navigating to the OpenScape SBC Assistant / OpenScape Branch Assistant tab.
- If OpenScape SBC Assistant / OpenScape Branch Assistant is informed by the License Management service that an RLF license file has expired, the OpenScape SBC Assistant / OpenScape Branch Assistant will return values of zero for all licenses whenever a device requests a license update. This will occur until a new license file is applied.

6.2 OpenScape Software Subscription License File

OpenScape SBC Assistant and OpenScape Branch Assistant support Software Subscription License (SSL) files. Software Subscription Licensing consists of two parts – the Product Instance and the Subscription License.

Licensing Structure

- **Product Instance**: The Product Instance is purchased once for each product and consists of all of the licenses necessary to equip a product for its maximum capacity, including all major features. The Product Instance is time limited each year until January 31st so the customer must renew their Product Instance annually between the first of December and the end of January. This does not require any additional ordering – just an update of the product license keys.
- **Subscription License**: The Subscription License is the monthly charge for a single user to use a single product. If a single OpenScape Branch user has voice, voice mail and Unified Communications (UC), then they would pay for 4 Subscription Licenses – one for OpenScape Voice, one for Xpressions, one for OpenScape UC and one for OpenScape Branch. The Subscription Licenses are based upon the product usage that is reported monthly and the billing is calculated on actual service consumption.

SSL License Customers

There are two SSL License Customer types; Service Providers and Enterprise customers. Service Providers resell OpenScape product, while Enterprise customers are end users. The following SSL licensing is provided based on the Licensing Structure and type of Customer:

- **Product Instance** - The following licenses are provided via SSL Licensing:
  - OpenScape Session Border Controller V8Product Instance for Service Provider Licensing
  - OpenScape Session Border Controller V8 Product Instance for Enterprise Licensing
- **Subscription License**- The following licenses are provided via SSL Licensing:
  - Monthly Subscription License Service Provider OpenScape Session Border Controller Session License (per session)
  - Monthly Subscription License Enterprise Provider OpenScape Session Border Controller Session License (per session)

License Functionality

- The OpenScape Branch Software Subscription licenses provide the capability for a customer to use OpenScape Branch functionality, including Branch base features, Branch Users, Auto Attendant feature, Backup ACD feature for the length of the software subscription.
- The OpenScape Session Border Controller (SBC) Software Subscription licenses provide the capability for a customer to use OpenScape SBC functionality, SBC base features and SBC sessions for the length of the software subscription.

License Monitoring

- The OpenScape SBC Assistant and OpenScape Branch Assistant display a popup at least once a day whenever any license file is within 60 days of expiration and whenever configuration is not possible due to the inability to check-out a license. The popup is displayed when navigating to the OpenScape SBC Assistant and OpenScape Branch Assistant.
- If OpenScape SBC Assistant and OpenScape Branch Assistant are informed by the License Management service that a Regular License File (RLF) license file has expired, the OpenScape SBC Assistant / OpenScape Branch Assistant will return values of zero for all licenses whenever a device requests a license update. This will occur until a new license file is applied.

License Billing

- OpenScape SBC Assistant and OpenScape Branch Assistant provide high water mark counters for the last 12 months and supports the retrieval of the current values of the high watermarks by the Common Management Platform (CMP) for each new license type.
- The billing period ID as well as the values of all high watermarks are included in the results.
- A high watermark of the values of the OpenScape SBC and OpenScape Branch License usage counters are calculated on every counter change and written to OpenScape SBC Assistant / OpenScape Branch Assistant database and the disk along with the billing period ID.
- On a monthly basis, the high watermarks are reset to the instant value of used Dynamic Licenses.
- The Software Subscription licensing related parameters/counters are displayed in the OpenScape SBC Assistant / OpenScape Branch Assistant.

Software Subscription License Monitoring and Reporting

- A monitoring and reporting mechanism resides in the OpenScape SBC Assistant, OpenScape Branch Assistant and CMP License Management Server for support of Software Subscription Licensing (SSL).
- OpenScape Branch Assistant provides calculation and reporting of OpenScape Branch User and OpenScape SBC Assistant provides calculation and reporting of OpenScape SBC Session license usage.

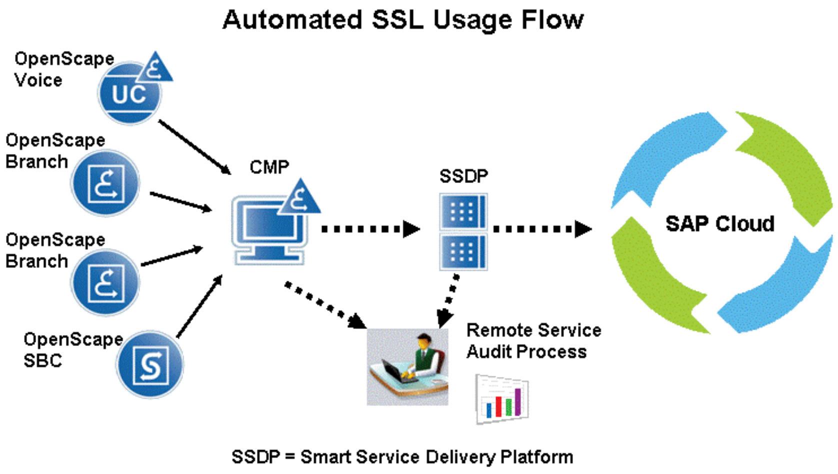
6.2.1 OpenScape Software Subscription License (SSL) Monitoring and Reporting - Details (OSB and SBC)

OpenScape Branch Assistant supports Software Subscription License (SSL) files with monitoring and reporting capabilities in Version 7 and beyond.

NOTICE: Note that in V8 the collection and reporting support of the SSL license counters (including those for OpenScape SBC) continue to be with the OpenScape Branch Assistant, i.e. the support for SBC related SSL counters is not relocated to the newly introduced OpenScape SBC Assistant.

Application Scenario

All of the products in the Software Subscription Licensing Model record subscriber license usage over the course of the month and allow this usage information to be retrieved by the CMP. “Usage” is defined as license consumption, based on the product’s current licensing model, not minute-by-minute usage of any particular product. The Smart Service Delivery Platform (SSDP) service tool provides remote access to the CMP for retrieval of the usage information by Unify. This usage information can be retrieved by SAP. The SSDP tool has the ability to schedule the automatic retrieval of the usage information, reducing the Unify Service overhead.



Terms and Definitions

- **High Water Mark**: As high watermark is defined the maximum value which is set. Any increment which produces a current value numerically greater than the current “high watermark”, should cause the “high watermark” to increase to the current value.

- **Billing Period**: As billing periods, in the context of Software Subscription Licensing, are defined monthly time intervals. The billing period ID is the number of the month where the billing period starts. The day of the month where a billing period starts is 1 e.g. Billing Period #1 is from January 1st 0:00:00 to January 31st 23:59:99.
- **Collection**: The SSDP periodically connects to the CMP and collects the usage data for the products (pull from CMP). Remote Service Engineer can display Monthly Usage for specific customer.
- **Billing**: The information gathered by SSDP and the customer ID are retrieved by SAP to invoice the customer for the monthly usage (pull from SSDP).

Description

- **Polling**: Once per day, each product is polled by the CMP for its usage (pull from product).
- **Display**: The CMP has a “Usage” screen that shows the monthly usage from all of the products.
- **Collection**: The SSDP periodically connects to the CMP and collects the usage data for the products (pull from CMP). Remote Service Engineer can display Monthly Usage for specific customer.
- **Billing**: The information gathered by SSDP and the customer ID are retrieved by SAP to invoice the customer for the monthly usage (pull from SSDP).
- **Usage**: Each product will calculate the usage based on their existing licensing model of either statically configured license usage or concurrent usage. For example, licensing in OpenScape Voice is a concurrent model where licenses are pulled from a pool for consumption based on the number of phones and soft clients currently registered. In contrast, OpenScape UC would use a statically configured model as licenses are consumed when a user is configured in the system, whether they login to OpenScape UC or not.
- **OpenScape Branch User Usage:**
  - For the OpenScape Branch User the usage is calculated based on the statically configured license usage.
  - OpenScape Branch User usage is defined as the high watermark for the number of consumed OpenScape Branch Registered Lines licenses in the month.
- **OpenScape SBC Session Usage**:
  - For the OpenScape SBC Session usage a “mixed” model is followed. The usage on the OpenScape Branch is calculated based on the statically configured license usage, while the usage on the OpenScape SBC is calculated based on the concurrent usage
  - As OpenScape SBC Session usage is defined as the high watermark of the number of consumed OpenScape SBC Session licenses in the month.

CMP License Management Service

The CMP License Management service is aware of the OpenScape Branch/ SBC related configured licenses. Thus the usage of the licenses where the statically configured model will be followed is retrieved by the CMP License Management Service.

Additionally the Product Instance ID (retrieved by the license file) is provided. The CMP License Management Service interface is called by OpenScape Branch Assistant whenever SSL usage data is reported to the SSL service.

CMP License Management service updates the a usage counter for the following:

- Whenever a modification is done in the number of the total configured OpenScape Branch Registered Lines licenses. If the modified number of total configured licenses is greater than the usage counter then the usage counter is updated, otherwise the usage counter remains unchanged.
- Whenever the Billing Period (the month) is changed. The first day of a month CMP License Management service resets the usage counter to the current value of the corresponding license counter.

NOTICE: The counter is stored encrypted to avoid unwanted modifications. Additionally, this counter is referred to the current Billing Period. The calculation of the Billing period is based on the configured system time of the application server (where CMP License Management Service is installed).

OpenScape Branch Assistant - Calculation of OpenScape SBC Session Usage

OpenScape Branch Assistant maintains one counter for the OpenScape SBC Session Usage for all the configured OpenScape Branch/SBC appliances. Usage is calculated separately on the OpenScape Branch appliances and the OpenScape SBC appliances and is combined into one count.

- Usage for OpenScape Branch (based on the statically configured model): Is the maximum of the total of the configured OpenScape SBC Sessions on all the configured OpenScape Branch appliances.
- Usage for OpenScape SBC (based on the concurrent model): Is the high watermark of the sum of the OpenScape SBC sessions simultaneously actually used for all the configured OpenScape SBC appliances.
- The final usage counter that is reported for the OpenScape SBC Session License shall is the sum of the usage on the OpenScape Branch plus the usage on the OpenScape SBC.

NOTICE: The counters are stored encrypted to avoid unwanted modifications. Additionally, those counters are referred to the current Billing Period. The calculation of the Billing period is based on the configured system time of the application server (where CMP License Management Service is installed).

The OpenScape Branch Assistant updates the a usage counter for the following:

- Whenever an update is done in the total configured OpenScape SBC sessions (case of OpenScape Branch) or in the number of the simultaneously actually used OpenScape SBC sessions (case of OpenScape SBC). If the updated number is greater than the usage counter then the usage counter is updated, otherwise the usage counter remains unchanged.

- Whenever the Billing Period (the month) is changed. The first day of a month OpenScape Branch Assistant resets the usage counter to the current value of the corresponding counter.

NOTICE: In case of redundant systems, OpenScape Branch Assistant takes into consideration only the licenses of the Master Node.

OpenScape Branch Assistant License Management Interface with the SSL Service

OpenScape Branch Assistant uses the interface of the SSL service in order to report the SSL usage data. Whenever the SSL service requests SSL usage data (e.g. once per day), OpenScape Branch Assistant performs the following:

- retrieves the usage counter of the OpenScape Branch User from the License Management service.
- reports the SSL usage counters for OpenScape Branch User and OpenScape SBC session to SSL service.
- request license information (OpenScape SBC Session usage included) from the OpenScape SBC appliances.
- reports the SSL usage counters for OpenScape Branch User and OpenScape SBC session to SSL service

The OpenScape Branch Assistant reports the following parameters to the SSL service:

Parameter	Description	Length	Allowed Characters
Year	The year the license info is reported. 4-digits representing the year (e.g. 2010).	4 characters	numeric only
Month	The month the license info is reported. Integer value ranging from 1 (January) to 12 (December).	2 characters	numeric only
Product-instance-ID	The unique ID of the product instance. This ID identifies the product in the SAP	17 characters	Alpha-numeric
Product Name	The name of the product (for informational purposes only).	20 characters	Alpha-numeric
Feature –ID (= License ID)	The ID of the feature (SSL Feature ID). Possible values depend on product type.	20 characters	Alpha-numeric

Parameter	Description	Length	Allowed Characters
Used-licenses	Number of used licenses in the reported month (High Watermark). If the CMP did not receive data from the product during the month, then -1 is reported.	6 characters	numeric only
Timestamp	Time when the last license update from the product was obtained. The Timestamp is used by SAP to determine up to date data was recieved for the month. This shall be reported as a string with format: yyyy-mm-dd hh:ss	16 characters	numeric plus “-“ and “:” charters
Violation	The violation flag indicates whether the license of the affected product is violated.	1 characters	true / false

In addition, OpenScape Branch Assistant reports the following parameters necessary to process SSL usage data within the CMP SSL service:

- Node name, string -The IP address or node name
- Node type, string - OpenScape Branch Assistant
- SSL Node Group - N/A (an empty string)

The additional parameters are not needed for SAP.

6.3 OpenScape Evaluation License File (SBC and OSB)

OpenScape SBC Assistant and OpenScape Branch Assistant support Evaluation License files. The Evaluation license file is a Regular License file (RLF) that expires after 180 (calendar) days.

License Functionality

- The OpenScape Branch Evaluation license file provides the license types and quantities necessary for a customer to evaluate OpenScape Branch functionality, including Branch base functions, Branch Users, Auto Attendant feature, Backup ACD feature for up to 180 days.
- The OpenScape Session Border Controller (SBC) Evaluation license file provides the license types and quantities necessary for a customer to evaluate OpenScape SBC functionality, SBC base functions and SBC sessions for up to 180 days.

License Monitoring

- OpenScape SBC Assistant and OpenScape Branch Assistant display a popup at least once a day whenever any license file is within 60 days of expiration and whenever configuration is not possible due to the inability to check-out a license. The popup is displayed when navigating to the OpenScape SBC Assistant / OpenScape Branch Assistant.

- If OpenScape SBC Assistant / OpenScape Branch Assistant is informed by the License Management service that an Evaluation license file has expired, the OpenScape Branch Assistant will return values of zero for all licenses whenever a device requests a license update. This will occur until a new license file is applied.

6.4 OpenScape Branch Base License Type (OSB only)

The OpenScape Branch Base license type provides full usage of the basic switch software.

The OpenScape Branch Base license type is not tied to a software release or hardware type. OpenScape Branch Base licenses are used to track the number of OpenScape Branch(s) in the field.

OpenScape Branch Base licenses are configured via the OpenScape Branch Assistant. The OpenScape Branch Assistant will then request the license from the existing License Management Service. If the OpenScape Branch Base licenses are not available, the OpenScape Branch Assistant will not allow the configuration of the Base License. The OpenScape Branch Assistant keeps track of the usage counters and displays the OpenScape Branch Base licenses assigned to OpenScape Branch devices.

An OpenScape Branch Base License is required for the following Branch types:

- OpenScape Branch - Proxy
- OpenScape Branch - SBC Proxy
- OpenScape Branch - Proxy ACD
- OpenScape Branch - Proxy ATA
- OpenScape Branch - Branch SBC

The maximum number of OpenScape Branch base licenses in a license file on the CMP is 3,000.

One OpenScape Branch Base License must be allocated and assigned to each OpenScape Branch managed by the CMP

6.5 OpenScape Branch Registered Lines LicenseType (OSB only)

Branch Registered Lines licenses control the number of lines that can register with an OpenScape Branch.

NOTICE: Prior to V8 these licenses were called OpenScape User Licenses. The name was changed to more accurately describe the purpose and enforcement criteria of these licenses

The OpenScape Branch Registered Lines license type is not tied to a software release or hardware type. OpenScape Branch Registered Lines licenses are used to track the number of systemwide OpenScape Branch Users.

OpenScape Branch Registered Lines licenses are configured via the OpenScape Branch Assistant. The OpenScape Branch Assistant will then request the license from the existing License Management Service. If the OpenScape Branch Registered Lines licenses are not available, the OpenScape Branch Assistant will not allow the configuration of the Registered Lines license. The OpenScape Branch Assistant keeps track of the usage counters and displays the OpenScape Branch Registered Lines licenses assigned to OpenScape Branch devices.

One OpenScape Branch Registered Lines license is required for the registration of each line or device including phantom and secondary lines.

The number of Registered Lines licenses in the license pool determines the following:

- The number of primary, phantom and secondary lines that can be registered concurrently.

  Example: OpenScape Branch Keyset with 1 prime line, 1 phantom line and 1 secondary line would use 1 OpenScape Voice dynamic license and 3 OpenScape Branch Registered Lines licenses.
- The number of non-keyset DNs that can have one or more telephones/soft clients simultaneously registered on the system. One OpenScape Branch Registered Lines license per registration request and one OpenScape Voice dynamic license per unique DN.

> **NOTICE:** Licenses that are purchased or included with a particular package only become available on the OpenScape Branch server when the license file is applied to the OpenScape Branch Assistant server and configured for the OpenScape Branch server. Until then, only the default number of licenses will be available on the OpenScape Branch server.

Upon SIP registration, the user is granted a single license from the pool of available licenses allocated to the OpenScape Branch server based on the rules stated above.

OpenScape Branch warning threshold occurs, as follows:

- If the Registered Lines licenses allocated exceeds the configurable warning threshold (e.g. 80% of the assigned licenses), a warning is generated to the customer’s system administrator. At this point, purchasing additional licenses may be necessary to provide a margin of safety.

Attempt to exceed user licensing:

- The number of allowed registrations is the number of Registered Lines licenses + 10% for 1000 Registered Lines licenses or less. The number of allowed registrations is the number of Registered Lines licenses + 5% for over 1000 Registered Lines licenses. Attempts to exceed these amounts will result in blocked registrations and a critical alarm is generated daily with text indicating registration(s) blocked due to insufficient Registered Lines licenses. The alarm must be manually cleared.
- Registration is on a first come first served basis

Users may reside in the following Branch types:

- OpenScape Branch - Proxy

- OpenScape Branch - SBC Proxy
- OpenScape Branch - Proxy ACD
- OpenScape Branch - Proxy ATA
- OpenScape Branch - Branch SBC
- Remote 3rd party Branch device

After enforcement is initiated and the license pool is completely depleted by the number of incoming SIP registered users, the next endpoint is denied registration and is unable to originate or terminate calls, including emergency calls.

6.6 OpenScape Branch Auto Attendant License (OSB only)

An OpenScape Branch Auto Attendant license allows access to Auto Attendant features.

Auto Attendant feature licenses are configured via the OpenScape Branch Assistant. An Auto Attendant feature license is optional and need not be purchased if Attendant functionality is not required.

The maximum number of Auto Attendant licenses is 1 per OpenScape Branch - Proxy ACD.

6.7 OpenScape Branch Backup ACD (Automatic Call Distribution) License (OSB only)

OpenScape Branch Backup ACD licenses control access to the ACD backup communication links feature provided during survivability processing.

Backup ACD feature licenses are configured via the OpenScape Branch Assistant. A Backup ACD feature license is optional and need not be purchased if ACD Backup functionality is not required.

The maximum number of Backup ACD licenses is 1 per OpenScape Branch - Proxy ACD.

6.8 OpenScape Session Border Controller (SBC) Base License (SBC only)

The OpenScape Session Border Controller (SBC) Base license provides full usage of the basic SBC software for a given version e.g. OpenScape SBC V2 base software.

The OpenScape SBC Base license is not tied to a software release or hardware type. OpenScape SBC Base licenses are used to track the number of OpenScape SBC(s) in the field.

OpenScape SBC Base licenses are configured via the OpenScape SBC Assistant. The OpenScape SBC Assistant will then request the license from the Existing License Management Service. If the OpenScape SBC Base licenses are not available, the OpenScape SBC Assistant will not allow the configuration of the Base License. The OpenScape SBC Assistant keeps track of the usage counters and displays the OpenScape SBC Base licenses assigned to OpenScape SBC devices.

The maximum number of OpenScape SBC base licenses in a license file is 100.

One OpenScape SBC Base License must be allocated and assigned to each OpenScape SBC managed by the CMP

6.9 OpenScape SBC Session License (SBC and OSB)

OpenScape SBC Session licenses are shared between OpenScape Branch and OpenScape SBC, and control the maximum number of connections to OpenScape SBC and OpenScape Branch SBCs.

OpenScape SBC Session licenses are configured via the OpenScape SBC Assistant and the OpenScape Branch Assistant. The OpenScape SBC Assistant / OpenScape Branch Assistant will then request the licenses from the existing License Management Service. If the OpenScape SBC Session licenses are not available, the OpenScape SBC Assistant will not allow the configuration of the Session License. The OpenScape SBC Assistant / OpenScape Branch Assistant keeps track of the usage counters and displays the OpenScape SBC Session licenses assigned to OpenScape SBC devices and OpenScape Branch SBC devices.

An OpenScape SBC Session License is required for the following:

- OpenScape SBC - Internet connections
- OpenScape SBC - SIP Trunking and Remote Subscribers
- OpenScape Branch - SBC Proxy - SIP Trunking
- OpenScape Branch - Branch SBC - SIP Trunking

The maximum number of OpenScape SBC Session licences is 200,000 (160K for OpenScape Branches and 40K for OpenScape SBCs).

6.10 OpenScape SBC Session Licenses

OpenScape SBC Session licenses are either shared between OpenScape Branch and OpenScape SBC, and control the maximum number of connections to OpenScape SBC and OpenScape Branch SBCs or are used for each trunk session or each user session connected.

OpenScape SBC Session licenses are configured via the OpenScape SBC Assistant. The OpenScape SBC Assistant will then request the licenses from the existing License Management Service. If the OpenScape SBC Session licenses are not available, the OpenScape SBC Assistant will not allow the configuration of the Session License. The OpenScape SBC Assistant keeps track of the usage counters and displays the OpenScape SBC Session licenses assigned to OpenScape Branch SBC and OpenScape SBC devices.

An OpenScape SBC Session License is required for the following:

- OpenScape SBC - Internet connections
- OpenScape SBC - SIP Trunking and Remote Subscribers
- OpenScape Branch - SBC Proxy - SIP Trunking
- OpenScape Branch - Branch SBC - SIP Trunking

The maximum number of OpenScape SBC Session licences is 200,000 (160K for OpenScape Branches and 40K for OpenScape SBCs).

6.11 Upgrade License - Overview

The OpenScape Upgrade Licenses are required when upgrading from an OpenScape Branch with pre-Version 2 software to an OpenScape Branch with Version 2 or later software; and is also required when upgrading from an OpenScape SBC with pre-Version 2 software to an OpenScape SBC Version 2 or later.

The enforcement of OpenScape License files begins with OpenScape Branch Version 2 and OpenScape SBC Version 2.

For SSL upgrade licenses are not required. Monthly Subscription licenses are version–independent. To upgrade from one major version to the next, a new Product Instance for the new product version is ordered (a small handling fee is charged) and the license file will deliver once again the full complement of feature and user licenses. The end user is invoiced for the monthly usage as usual and the change is transparent to the user.

Licensing Software Upgrades for the OpenScape Branch and OpenScape SBC

The following applies to handling of software upgrades for OpenScape Branch and OpenScape SBC:

- OpenScape Branch Assistant upgrade from a version that does not support licensing to a version (including V8 which includes the separate OpenScape SBC Assistant appearance) that does support licensing:
  - Prior to upgrading an OpenScape Branch or OpenScape SBC device in a customer network to a software release that supports OpenScape licensing, the OpenScape Branch Assistant must be upgraded to a revision that provides provisioning of OpenScape Branch and OpenScape SBC Licenses. If the OpenScape Branch Assistant in not upgraded, then licensing of Branch or SBC via Common Management Platform (CMP) is not possible. Stand Alone licensing must be used directly on the Branch or SBC.
  - The OpenScape Branch Assistant must be provisioned with the OpenScape Branch and OpenScape SBC licensing information; otherwise, the OpenScape devices will not allow licensed features to work when the OpenScape Branch or OpenScape SBC devices are upgraded and start requesting licensing information. A license file, generated with the MAC ID of the Assistant, must be applied to the Assistant.
- OpenScape Branch Assistant upgrade (includes OpenScape SBC Assistant in V8) from a version that does support licensing:
  - OpenScape Branch and OpenScape SBC license data must be maintained whenever the OpenScape Branch Assistant is upgraded.
- After performing an OpenScape Branch or OpenScape SBC software upgrade from a release that did not support OpenScape Branch or OpenScape SBC licensing to a release that does support licensing, the

OpenScape Branch or OpenScape SBC device will begin requesting licenses automatically.

- When performing an OpenScape Branch or OpenScape SBC software upgrade from a release that does support OpenScape Branch or OpenScape SBC licensing to a newer release, the upgrade is performed as usual and the device will begin to request its licenses automatically when it reconnects to the network.
- When performing an OpenScape Branch or OpenScape SBC software upgrade from a release with a license version 8 or older, it will be necessary to request a new license file for version 10. In the latest V10R2, the upgrade will abort with an error message saying that the current license version (V8 or older) is not allowed to do an upgrade. In case of a full installation, the old license file will be rejected during the license upload. Only V9 or later licenses are accepted in the latest V10R2.

NOTICE: If the license file version is V8 or older but the license file contains the component id "EMSS_Check" (Extended Manufacturer Software Support) which is still valid, the upgrade procedure will be executed, and the license file will be accepted.

OpenScape Branch Upgrade Licenses

The following Upgrade Licenses apply to OpenScape Branch:

- OpenScape Branch V9 Upgrade Base from Branch V1
- OpenScape Branch V9 Upgrade User from Branch V1
- OpenScape Branch V9 Upgrade Auto Attendant License from Branch V1
- OpenScape Branch V9 Backup ACD License from V1
- OpenScape SBC V9 Upgrade Session License from SBC V1

OpenScape SBC Upgrade Licenses

The following Upgrade Licenses apply to OpenScape SBC:

- OpenScape SBC V9 Upgrade Base License from SBC V1
- OpenScape SBC V9 Upgrade Session License from SBC V1

6.12 Managing Licenses

This chapter provides information about the following topics:

- License Management Concept
- License Information
- Activating Licenses

6.12.1 License Management Concept

The legal use of the OpenScape system features requires the corresponding product licenses. You can use the license management to activate these licenses and to view license information. The license management works domain-spanning.

Central License Server (CLS) The Central License Server (CLS) generates and manages the license files. A license file is generated when the License Authorization Code is sent to the CLS by Common Management Platform. The transfer of the license file to Common Management Platform occurs automatically via the internet.

IMPORTANT: When you connect the Common Management Platform computer system to the internet, make sure that the computer system can only connect to the CLS and other selected, secure target systems.

NOTICE: In certain circumstances the Common Management Platform may not be able or desired to access the internet. In this case it is possible to manually generate the license file at the CLS and to download it. The associated licenses can then be activated in the Common Management Platform with the license file alone and without internet connection (offline activation).

Every customer or sales partner has a separate license account on the CLS. The accounts can be maintained at the CLS via a separate web-based user interface. All available and already purchased licenses can be displayed.

Centralized Licensing via Common Management Platform

Centralized Licensing implies that the license file is applied at the Common Management Platform (CMP). The license file must have been generated previously with the MAC ID of the CMP. This license file can be offline activated/ applied via the CMP. Optionally, a License Authorization Code (LAC) can be used to online activate/apply a license file via the CMP.

The licenses are applied/activated with Common Management Platform either offline or online. The Common Management Platform online activation transfers the License Authorization Code (LAC) to the CLS and receives the associated license file. The CMP offline activation assumes the license file was previously generated (with the CMP MAC ID).

The licenses and their related information are displayed in Common Management Platform. The total number of licenses, which licenses are assigned to which OpenScape Branches or OpenScape SBCs, and when these licenses expire can be viewed in the CMP. In addition, number of licenses that are still free can also be viewed.

OpenScape Branch Assistant stores licensing information encrypted on the disk.

Licensing in Stand Alone Mode

Stand Alone Mode is defined as when an OpenScape Branch or OpenScape SBC is deployed at a customer who does not have a Common Management Platform (CMP) with OpenScape Branch Assistant (or OpenScape SBC Assistant) or the CMP is not upgraded to a version that supports OpenScape Branch licensing. The standalone license file must have been previously generated and supplied to the customer, using the MAC ID of the OpenScape

Branch or SBC. These customers use the OpenScape Branch or OpenScape SBC local GUI to manage the OpenScape Branch or OpenScape SBC.

Grace Period

After purchasing or installing the product/feature, the license for it must be activated within a specified time period - called the grace period. Depending on the product involved, this period may be e. g. 30 days.

During this grace period, the product may be restricted or fully functional. If you do not install a license after the grace period, the product becomes severely restricted or stops working entirely.

MAC address (Locking-ID)

During production, hardware is assigned a board-specific number called a MAC address which is unique world-wide. To guarantee unique licensing, the license file is linked to the hardware's MAC address (for example, network card of the system server). Every project/feature license is therefore linked to this locking ID.

6.12.2 License Information

This Common Management Platform (CMP) and the OpenScape SBC Assistant and OpenScape Branch Assistant can be used to retrieve licensing information:

License Information via Common Management Platform (CMP)

The following information can be displayed using the CMP:

- **General license information**

  The general license information contains

  – the license name (feature name)
  – the name of the product for which the license is used
  – the number of licenses already used
  – the licenses validity
- **License locking IDs**

  A locking ID is a unique feature of a computer system - e. g. the MAC address of a network board. The purchased licenses are linked to the locking ID. You may have to select a locking ID to which you want to bind licenses the first time you license the system. All further licensing activities are performed with this locking ID.
- **Software Subscription License Monitoring and Reporting**

  OpenScape CMP supports display of Software Subscription License (SSL) information in Version 7 and beyond. Starting in V8 the OpenScape SBC Assistant also displays the SBC specific SSL information.

License Information via OpenScape SBC Assistant and OpenScape Branch Assistant

The following information can be displayed:

- **General license information per Branch or SBC**

  The general license information contains

  - the node name
  - the license type
  - the number of licenses configured
  - the number of licenses locally configured
  - the peak number of licenses used during the past month
  - when the license was first updated to the Branch or SBC
  - when the license was last updated to the Branch or SBC
- **License thresholds**

  License thresholds can be set and displayed for the following license types:

  - OpenScape Branch Base
  - OpenScape SBC Base
  - OpenScape Branch Users
  - Auto Attendant feature
  - Backup ACD feature
  - SBC Sessions

  The percentage threshold for each license type is used to warn the customer that more licenses may need to be purchased. When the percentage of licenses have been allocated from the license pool, a pop-up warning will be issued indicating that threshold was exceeded.

6.12.2.1 How to Display License Information via CMP

To display license information via the Common Management Platform (CMP), proceed as follows:

Prerequisites

Adequate administrative permissions.

Step by Step

1) On the **Maintenance** navigation tab click on the **License** navigation menu item.
2) Select **Information** in the navigation tree.

3) A list of all features available in the OpenScape system is displayed in the work area. This list contains for each entry the following information:

Product Name

Shows the name of the product for which the license information is being displayed e.g., OpenScape Branch / SBC V2.

Feature Name

States the feature name/license type associated with the product e.g., OpenScape SBC Base.

Number of used licenses

Specifies how many licenses are altogether available for the feature and how many of these are already used e.g., 1 of 30.

Validity

Shows the validity for the feature's licenses by expiration date. License entries that are invalid or have expired or are about to expire are marked red e.g., Grace Period 30 days, or unlimited.

4) The list can be filtered according to specific terms (patterns).

a) Enter the desired filter term in the field Pattern. You can either enter the complete term or the initial letters followed by * (e. g. *HiPath*).

b) From the list displayed, select whether the filtering is to be applied to the Product Name or Feature Name column.

c) Click on **Go** to activate the filter. Only the list elements which correspond to the pattern entered are displayed.

d) Click on **Clear** to deactivate the filter. Filter conditions are deleted. All the list elements are displayed again.

5) Information in the list can be exported to a CSV file.

a) Click the **CSV icon** in the work area to the right of the Items/Page controls.

b) From the File Download dialog select **Save**.

c) Enter the **Save in:** location and **File Name** and click on **Save**.

d) The CSV file is saved and the **License Information** work area appears.

6.12.2.2 How to Display Software Subscription License Information via CMP

To display Software Subscription License (SSL) data via the Common Management Platform (CMP), proceed as follows:

Prerequisites

Adequate administrative permissions.

Step by Step

1) On the **Maintenance** navigation tab click on the **License** navigation menu item.

2) Select **Software Subscription** in the navigation tree.

The Subscription License Usage dialog appears.

3) A list of nodes by name and type with the associated subscription licenses is displayed in the work area. This list contains for each entry the following information:

Node Name

Shows the name of the node for which the license information is being displayed e.g., bocaosb1.

Node Type

Indicates the type of node associated with subscription license reported e.g., OpenScape Branch, OpenScape Branch/SBC.

License Type

Indicates the type of subscription license reported e.g., OpenScape Branch User, OpenScape Branch Session.

Quantity

Shows the number of used licenses in the reported month (High Watermark). If the CMP did not receive data from the product during the month, then -1 is reported.

Product ID

The unique ID of the product instance. This ID identifies the product in the SAP.

Remaining Days

Shows the number of days left in the subscription licenses for the node. e.g., 155 days.

Collection error

The Collection error flag indicates there was an issue with collection of license data.

Last collection date

When the last license update from the product was obtained. The Timestamp is used by SAP to determine up to date data was received for the month.

4) The list can be filtered according to specific terms (patterns).

a) Enter the desired filter term in the field Pattern. You can either enter the complete term or the initial letters followed by * (e. g. *HiPath*).

b) From the list displayed, select whether the filtering is to be applied to the Node Type or Product ID.

c) From the year and month field list, select the year and month for which the data will be displayed.

NOTICE: Data is only valid for a rolling year.

d) Click on **Search** to activate the filter. Only the list elements which correspond to the pattern entered are displayed.

e) Click on **Show all** to deactivate the filter. Filter conditions are deleted. All the list elements are displayed again.

5) Information in the list can be sorted by Node Name, Node Type and Violation by clicking the associated column name.

6.12.2.3 How to Display License Locking IDs via CMP

To display license locking IDs via the Common Management Platform (CMP), proceed as follows:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **License** navigation menu item.

2) Select **Locking IDs** in the navigation tree.

3) A list of all computer systems available in the entire system is displayed in the work area. This list contains for each entry the following information:

> **NOTICE:** If a Locking ID was already used for licensing, it is the only Locking ID displayed.

Locking ID

Shows the Locking ID (MAC address) of the system to which the licenses are registered.

Adapter Name

Shows the name of the adapter that provides the Locking ID.

Logical Name

Specifies the logical name of the adapter that provides the Locking ID.

IP Address

Specifies the IP address of the adapter that provides the Locking ID. Here there could be several IP addresses displayed - such as in server scenarios. or no IP address (adapter out of service).

4) If access to the central license server is required, click **Link to the Central License Server**.

6.12.2.4 How to Display License Information via OpenScape SBC Assistant and OpenScape Branch Assistant

To display license information via the OpenScape SBC Assistant or OpenScape Branch Assistant, proceed as follows:

Prerequisites

Adequate administrative permissions.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape Branch** or **OpenScape Branch** within the Navigation Bar in the Common Management Platform.

2) Select **Licensing** in the navigation tree, under Administration.

3) Select **Licensing list** in the navigation tree, under Licensing.

4) A list of all licenses available for OpenScape Branches, OpenScape Branch application features and OpenScape SBCs are displayed in the work area. This list contains for each entry the following information:

   Name

   Shows the name of the OpenScape Branch or OpenScape SBC for which the license information is being displayed.

   License Type

   Type of Licenses are as follows:

   - OpenScape Branch Base
   - OpenScape Branch Users
   - Auto Attendant feature
   - Backup ACD feature
   - SBC sessions
   - OpenScape SBC Base

   Configured licenses

   Specifies how many licenses are configured in the Assistant for this logical device.

   - OpenScape Branch Base (values - 0-1)
   - OpenScape Branch Users (values - 0-6000)
   - Auto Attendant feature (values - 0-1)
   - Backup ACD feature (values - 0-1)
   - SBC sessions (values - 0-4000)
   - OpenScape SBC Base (values - 0-1)

   Locally Configured licenses

   Specifies how many licenses are configured for this physical device, OpenScape Branch or OpenScape SBC. Maximum values are the same as Configured license values.

   Usage (Peak)

   Shows the peak number of licenses used for the current month.

   First updated

   Date and time when the license information was first updated between the CMP and OpenScape Branch or OpenScape SBC.

   Last updated

   Date and time when the license information was last updated between the CMP and OpenScape Branch or OpenScape SBC.

5) The Licences list can be filtered by Name.

   a) Enter the desired filter term in the field Pattern. You can either enter the complete term or the initial letters followed by * (e. g. *C-SBC*).

   b) Click on **Go** to activate the filter. Only the list elements which correspond to the pattern entered are displayed.

   c) Click on **Clear** to deactivate the filter. Filter conditions are deleted. All the list elements are displayed again.

6.12.2.5 How to Display and Manage Licensing Thresholds via OpenScape SBC Assistant or OpenScape Branch Assistant

This feature allows the administrator to manage the allocation of licenses by specifying the threshold values for licenses associated with OpenScape Branch and OpenScape SBC. The threshold value is used to determine when to generate a warning (pop-up) so the administrator can obtain additional licenses prior to running out of licenses. To display or manage threshold license information via the OpenScape SBC Assistant or OpenScape Branch Assistant, proceed as follows:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC or OpenScape Branch** within the Navigation Bar in the Common Management Platform.

2) Select **Licensing** in the navigation tree, under Administration.

3) Select **License thresholds** in the navigation tree, under Licensing.

The **OSB licenses thresholds** dialog opens. The SBC license threholds are shown when using the OpenScape SBC Assistant. The OSB license threholds are shown when using the OpenScape Branch Assistant.

4) The following Licenses and associated thresholds will be displayed

OpenScape Branch Base (%):

The default value is 80%, and the valid range is [0 % ...100 %].

OpenScape SBC Base (%):

The default value is 80%, and the valid range is [0 % ...100 %].

OpenScape Branch Users (%):

The default value is 80%, and the valid range is [0 % ...100 %].

Auto Attendant feature (%):

The default value is 90%, and the valid range is [0 % ...100 %].

Backup ACD feature (%):

The default value is 90%, and the valid range is [0 % ...100 %].

SBC Sessions (%):

The default value is 90%, and the valid range is [0 % ...100 %].

5) Enter the threshold percentage of licenses used for the associated license type(s). When the license usage reaches the threshold value a warning shall be sent to the administrator.

6) Click **Save** to make the changes of the threshold values valid.

The threshold warning level for the associated license type usage is modified and set.

6.12.2.6 How to Display Licensing for an OpenScape SBC Via OpenScape SBC Assistant

The OpenScape SBC Assistant can administer OpenScape SBCs. Thus it keeps a list of SBCs in its database. The "OpenScape SBC Overview" form displays all known SBCs and provides a search function to find a particular one. The administrator can select a single OpenScape SBC to view and configure.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) To display all SBCs offices: navigate to **Configuration tab** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select **All systems** in the **Communication System** pull-down under **Administration** in the Navigation Tree (if not currently selected).

   If **All systems** is not currently selected, selecting All systems will display the **OpenScape SBC Overview** in the Work Area, with a current list of all known SBCs of all systems. If no SBCs are defined, the list is empty. If **All systems** was previously selected, then proceed to step 3.

3) Select **OpenScape SBC list** in the Navigation Tree.

   The system presents the **OpenScape SBC Overview** in the Work Area, with a current list of all known SBCs of all systems. If no SBCs are defined, the list is empty.

4) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

5) To find and select a particular branch office use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC or branch office in the list. Action Menu buttons are set active in the Work Area with the following options: **Manage**, **Local Password...**, **Refresh Selected**, **Edit...**, **Delete**. Selecting the **Manage** button updates the **OpenScape SBC** field, in the Navigation Tree, with the selected SBC and displays information and data in the Work Area for that SBC.
   - Choose a SBC from the **OpenScape SBC Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
   - Enter filter search criteria to filter the list of SBC.

     Filtering is possible on the following criteria from the **in** field: **OpenScape SBC** (name), **Business Group, IP Address, Version, Status, Mode.**

     NOTICE: Wild cards are supported (* for 0 or more characters, "?" for single characters).

6) Once the filters are set, click the **Go** button.

   The system refreshes the list of displayed SBCs and displays the ones matching the search criteria.

7) Click The **Clear** button. The system clears the filter criteria field and displays all records of the default communication system selected in the **Communication System** field. If no specific communication system is selected, all SBCs of all systems are listed in the Work Area.

8) View the work area under **Licensing Information**. The following is displayed:

   First updated:

   Date and time when the license was first updated.

   Last updated:

   Date and time when the license was last updated.

   Logical ID:

   Unique ID for the OpenScape Branch or OpenScape SBC in the form of System Name:Business Group Name:OpenScape Branch or SBC Name.

   Hw ID:

   Unique Hardware ID associated with the hardware of the OpenScape Branch or OpenScape SBC.

   License type

   Type of Licenses are as follows: OpenScape Branch Base, OpenScape Branch Users, Auto Attendant feature, Backup ACD feature, SBC sessions and OpenScape SBC Base.

   Configured

   Specifies how many licenses are configured in the OpenScape Branch Assistant for this logical device.

   Locally Configured

   Specifies how many licenses are configured for this physical device, OpenScape Branch or SBC.

   Usage (Peak)

   Shows the highest number of licenses used at any point in time during the current month.

   Refresh button

   Used to refresh the current licensing information displayed for that particular OpenScape Branch or OpenScape SBC from the OpenScape Branch Assistant database.

   Device license update button

   Used to request an update of license data from the OpenScape Branch Assistant, to the OpenScape Branch or OpenScape SBC device.

   Configure button

   Used to access configuration of licenses for the OpenScape Branch or OpenScape SBC. In addition, provides access to clear license counters at the OpenScape Branch and SBC devices.

9) Configuration and update of licenses can be accomplished for a single OpenScape Branch Office or OpenScape SBC.

The data displayed is provided by the OpenScape Branch assistant database and the OpenScape Branch or SBC hardware itself. This means that the data might be out of date if it was changed on the SBC or branch office without the assistant being notified. Refresh button must be used to synchronize data when changes are made.

6.12.2.7 How to Configure and Clear Licensing for an OpenScape SBC Via OpenScape SBC Assistant

The OpenScape SBC Assistant can administer licensing for a particular OpenScape SBC.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Completed either online or offline license activation to apply the license file to the Common Management Platform (CMP).

Step by Step

1) To display all SBCs: navigate to **Configuration tab** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select **All systems** in the **Communication System** pull-down under **Administration** in the Navigation Tree (if not currently selected).

If **All systems** is not currently selected, selecting All systems will display the **OpenScape SBC Overview** in the Work Area, with a current list of all known SBCs of all systems. If no SBCs are defined, the list is empty. If **All systems** was previously selected, then proceed to step 3.

3) Select **OpenScape SBC list** in the Navigation Tree.

The system presents the **OpenScape SBC Overview** in the Work Area, with a current list of all known SBCs of all systems. If no SBCs s are defined, the list is empty.

4) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

5) To find and select a particular SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list. Action Menu buttons are set active in the Work Area with the following options: **Manage**, **Local Password...**, **Refresh Selected**, **Edit...**, **Delete**. Selecting the **Manage** button updates the **OpenScape SBC** field, in the Navigation Tree, with the selected SBC and displays information and data in the Work Area for that SBC.
- Choose an SBC from the **OpenScape** SBC pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- Enter filter search criteria to filter the list of SBC.

  Filtering is possible on the following criteria from the **in** field: **OpenScape SBC** (name), **Business Group, IP Address, Version, Status, Mode.**

  > **NOTICE:** Wild cards are supported (* for 0 or more characters, "?" for single characters).

6) Once the filters are set, click the **Go** button.

The system refreshes the list of displayed branch offices and displays the ones matching the search criteria.

7) Click The **Clear** button. The system clears the filter criteria field and displays all records of the default communication system selected in the **Communication System** field. If no specific communication system is selected, all SBCs of all systems are listed in the Work Area.

8) This Step should be executed when changing out OpenScape SBC hardware.

a) Click the **Configure** button in the work area under Licensing Information.

The **Configure licenses** licenses dialog appears and the following information is displayed:

- Clear license counters
- OpenScape licenses assigned for each license type
- Number of available licenses associated with each license type

b) Checkmark the **Clear license counters** and click the **Save** button to clear out “all” licenses at the OpenScape SBC device. This will clear the link between the allocated licenses and the hardware ID.

> **NOTICE:** This should be done prior to changing out OpenScape SBC hardware.

The licenses on the OpenScape SBC are cleared and the General OpenScape work area appears. The allocated licenses are not returned to the license pool.

c) Uncheck the **Clear license counters** checkbox and click the **Save** button once the new hardware is installed; the **Clear license counters** checkbox should be cleared so the new hardware can receive the licenses configured in the OpenScape SBC Assistant. This will link the licenses allocated to the device with the devices’ hardware ID.

The General OpenScape work area appears.

9) Enter the number of licenses to be assigned to the OpenScape SBC for each license type. The number of assigned licenses can not exceed the number of available licenses shown e.g., **Available:** 5017, for the associated license type. License types include the following:

- **SBC Sessions** (for Branch or SBC)
- **OpenScape SBC Base** (for SBC)

10) Click the **Save** button to complete the assignment of licenses in the OpenScape SBC Assistant for the OpenScape SBC device.

> **NOTICE:** This action also updates OpenScape SBC licenses in the OpenScape hardware.

> **IMPORTANT:** Applying or changing licenses assigned to an SBC will cause the SBC to restart the sip server process which will have an affect on transient (non-stable) calls.

Licenses are now allocated in the OpenScape SBC Assistant for the OpenScape SBC and the General OpenScape work area appears.

11) Click the **Device license update** button, in the Licensing Information work area to update license information in the OpenScape SBC device.

> **NOTICE:** This action transfers licensing information from the OpenScape SBC Assistant to the OpenScape SBC hardware.

Licenses are now configured in the OpenScape SBC hardware.

12) Click the **Refresh** button, in the Licensing Information work area to refresh the OpenScape SBC licensing information from the OpenScapeSBC Assistant only.

The data displayed is provided by the OpenScape SBC assistant database rather than the hardware itself. This means that the data might be out of date if it was changed on the SBC without the assistant being notified.

6.12.2.8 How to Display Licensing Warnings for an OpenScape SBC

The OpenScape SBC Assistant automatically displays licensing warnings to notify the administrator of possible licensing issues. Warnings can occur during display and configuration of OpenScape SBCs.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select **All systems** in the **Communication System** pull-down under **Administration** in the Navigation Tree (if not currently selected).

   If **All systems** is not currently selected, selecting All systems will display the **OpenScape SBC Overview** in the Work Area, with a current list of all known SBCs of all systems. If no SBCs are defined, the list is empty. If **All systems** was previously selected, then proceed to step 3.

3) Select **OpenScape SBC list** in the Navigation Tree.

The system presents the **OpenScape SBC Overview** in the Work Area, with a current list of all known SBCs of all systems. If no SBCs s are defined, the list is empty.

4) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

5) To find and select a particular SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list. Action Menu buttons are set active in the Work Area with the following options: **Manage**, **Local Password...**, **Refresh Selected**, **Edit...**, **Delete**. Selecting the **Manage** button updates the **OpenScape SBC** field, in the Navigation Tree, with the selected SBC and displays information and data in the Work Area for that SBC.
- Choose a SBC or branch office from the **OpenScape SBC** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- Enter filter search criteria to filter the list of SBC.

  Filtering is possible on the following criteria from the **in** field: **OpenScape SBC** (name), **Business Group, IP Address, Version, Status, Mode.**

> **NOTICE:** Wild cards are supported (* for 0 or more characters, "?" for single characters).

6) Once the filters are set, click the **Go** button.

The system refreshes the list of displayed SBCs and displays the ones matching the search criteria.

7) Click The **Clear** button. The system clears the filter criteria field and displays all records of the default communication system selected in the **Communication System** field. If no specific communication system is selected, all SBCs of all systems are listed in the Work Area.

8) Choose a particular OpenScape SBC.

OpenScape SBC associated information is displayed. In addition, licensing pop-up warnings will appear if applicable. Warning may include but are not limited to the following:

- A license file is within 60 days of expiring. If a new license file is not added within xx days branch calls will not be possible.
- A configured threshold has been exceeded.
- A license file has expired, calls will not be possible.
- A license file has been applied that does not have enough licenses. Add a new license file with sufficient licenses for the licenses configured in the Assistant.
- A configuration was attempted but no license was available
- Number of licenses according to the device is out of sync with the number of configured licenses (i.e. after the device responds with a status of “success” after updating its license info but the number of licenses the device reports to have is different than the number of licenses configured.

Note: this can happen if the administrator assigns more SBC Session licenses than the OpenScape SBC hardware can handle.

9) Warnings can occur during display and configuration of OpenScape SBCs.

The administrator is warned about licensing issues and can then correct the pending issue.

6.12.3 Activating Licenses

After you have purchased an OpenScape product, you will have to activate the licenses supplied with it in order to enable the product and its features.

Licenses can be activated by one of the following two methods:

In order to activate licensing via the Common Management Platform (CMP); the license file must have been generated using the MAC ID of the CMP.

NOTICE: If the CMP does not support licensing or no CMP is available, OpenScape Branch or OpenScape SBC licensing can be activate via the Stand Alone Licensing mechanism using the local administration GUI.

- **Activating a License Online with License Authorization Code**

  License activation via the LAC is the standard method. Using the LAC, a license file is generated at the Central License Server (CLS) and forwarded to the Common Management Platform. The license file is used to activate the associated licenses and thus release the products and their features.
- **Activating a License Offline with a License File**

  License activation with the license file is necessary if you cannot or do not want to perform online activation and if the license file is directly available. The license file was generated at the Central License Server (CLS) earlier and downloaded. The license file is used to activate the associated licenses and thus release the products and their features.

Supplementary licenses can be purchased to use additional products. When additional licenses are purchased, a separate License Authorization Code (LAC) is provided which can then be used to activate the new licenses you purchased. After activation, all features for which a license is required will be available.

Process Flow for Online License Activation (example)

1) The order is placed by the customer and entered in the SAP system, for example.

2) The license-relevant order details are stored in the database of the CLS.

3) The CLS automatically generates the license authorization code (LAC) from the data. This LAC is forwarded to the customer (for example, via e-mail) together with the CLS access data.

4) The delivery of the product/feature is initiated.

5) The customer installs the product/feature. The grace period begins during which the product/feature must be licensed.

6) The customer transfers the License Authorization Code to the CLS via the internet by using the Common Management Platform. Some customer-specific hardware data (such as the MAC address of the system server, which is also called the Locking ID) is sent to the CLS along with the LAC.

7) The CLS uses the License Authorization Code and the customer-specific hardware data to generate a license file and then sends this back to the Common Management Platform. The license file contains all the licenses associated with the product/feature.
8) The license management of the Common Management Platform checks if the MAC address saved in the license file matches the MAC address of the system server (locking ID). If the check succeeds, the licenses of the product/feature are added to the license pool of the CMP. Otherwise, the licenses are not added to the pool.
9) The customer can then create the OpenScape Branch or OpenScape SBC in the CMP and allocate licenses to the branch or sbc from the pool, to provide the functionality purchased.

6.12.3.1 How to Activate License - Online

Online license activation via the LAC (License Authorization Code) is the standard method. Using the LAC, a license file is generated at the Central License Server (CLS) and forwarded to the Common Management Platform. The license file is used to activate the associated licenses and thus release the products and their features.

Prerequisites

Adequate administrative permissions.

Common Management Platform and OpenScape SBC Assistant / OpenScape Branch Assistant version supports OpenScape SBC/Branch Licensing.

The license file must have been generated with the MAC ID of the Common Management Platform (CMP)

Step by Step

1) On the **Maintenance** navigation tab click on the **License** navigation menu item.
2) Select **Information** in the navigation tree.

> **IMPORTANT:** OpenScape Voice license activation is not offered via CMP.

3) Click the **Online Activation...** button in the work area.

   The **Activate licenses online** dialog appears.
4) Specify under License authorization code (LAC) the license authorization code you have received with the OpenScape product.
5) Select a locking ID under Locking ID. There is no selection option available if only one locking ID is present.
6) Enter the user name and password for accessing the license server under User name and Password.

> **NOTICE:** Certain products can also be anonymously licensed without a user name and password. Deactivate the **I would like to logon at the License Server with the**

following account option for this purpose. If you have a valid user ID for the license server you should use it for anonymous licensing also.

7) Click **Activate**.

The connection to the license server is established, and the license is released. As a rule, this operation does not take more than 90 seconds.

NOTICE: The license pool is created and licenses can then be allocated/configured to individual OpenScape Branches or OpenScape SBCs.

6.12.3.2 How to Activate License - Offline

License management can be used to import a new or updated license file offline. A license file is required which can be downloaded from the Central License Server (CLS). The license file is used to activate the associated licenses and thus release the products and their features.

Prerequisites

Adequate administrative permissions

The license file must have been generated with the MAC ID of the Common Management Platform (CMP)

Step by Step

1) On the **Maintenance** navigation tab click on the **Licenses** navigation menu item.
2) Select **Information** in the navigation tree.

   IMPORTANT: OpenScape Voice license activation is not offered via CMP.

3) Click the **Offline Activation...** button in the work area.

   The **License Activation** dialog appears.
4) Select on **Browse** next to the **License file** field and navigate to the storage location of the license file you have received with the product.
5) Click **Activate**.

The license management verifies the signature of the license file against the system server's MAC address (Locking ID). If the verification is successful, the data is transferred from the file and the licenses are displayed in the Common Management Platform with the associated information.

NOTICE: The license pool is created and licenses can then be allocated/configured to individual OpenScape SBCs.

6.12.4 License Enforcement and Update

This Common Management Platform (CMP) and the OpenScape Branch Assistant / OpenScape SBC Assistant (V8 forward) can be used to retrieve licensing information:

Enforcing Licensing

Alarms, pop-ups and logging will occur when enforcing licensing limits.

The following table shows how Licensing enforcement will be handled during Installation/Upgrade and when OpenScape devices are operational:

	Install / Upgrade License Enforcement	Operation License Enforcement
Base license	No base: No enforcement	No base: No enforcement
Registered Lines license (OSB only)	• If no Licenses of any type are available, operate as today but alarm daily. After 30 days of no licenses block all registrations. • If licenses of any type are provided during the 30 day period OpenScape Branch begins to operate based on the licenses available.	Attempts to exceed license: • The number of allowed registrations is the number of Registered Lines licenses + 10% for 1000 Registered Lines licenses or less. The number of allowed registrations is the number of Registered Lines licenses + 5% for over 1000 Registered Lines licenses. Attempts to exceed these amounts will result blocked registrations and a critical alarm is generated daily with text indicating registration(s) blocked due to insufficient Registered Lines licenses. The alarm must be manually cleared. • Registration is on a first come first served basis
SBC Session license (OSB and SBC)	• If no Licenses of any type are available, operates normal but alarm daily. After 30 days of no licenses the final response to Invites will be 606 (a warning header may be included for diagnostic purposes). The same is true for gateways. • If licenses of any type are provided during the 30 day period OpenScape Branch or OpenScape SBC begins to operate based on the licenses available.	Attempts to exceed license: • Established SIP Service Provider/ OpenScape SBC calls will be counted based on 2xx (ack) responses. New Invites exceeding the license limit will be rejected with response code 606 (a warning header may be included for diagnostic purposes) and a critical alarm is generated daily with text indicating SIP Service Provider calls blocked due to insufficient SBC Session licenses. The alarm must be manually cleared.
Attendant license (OSB only)	• If no Licenses of any type are available, operate normal but alarm daily. After 30 days of no licenses calls to the Attendant are not possible (all calls are blocked). • If licenses of any type are provided during the 30 day period OpenScape Branch begins to operate based on the licenses available.	Attempts to exceed license: • Reject calls to the Attendant with response code 606 (a warning header may be included for diagnostic purposes) and a critical alarm is generated daily with text indicating Attendant calls blocked due to no Attendant License. The alarm must be manually cleared.

	Install / Upgrade License Enforcement	Operation License Enforcement
Backup ACD license (OSB only)	• If no Licenses of any type are available, operate normal but alarm daily. After 30 days of no licenses calls going into the queue are not possible (all calls are blocked). • If licenses of any type are provided during the 30 day period OpenScape Branch begins to operate based on the licenses available.	Attempts to exceed license: • Reject calls to Backup ACD with response code 606 (a warning header may be included for diagnostic purposes) and a critical alarm is generated daily with text indicating Backup ACD calls blocked due to no Backup ACD. The alarm must be manually cleared.

- **Additional Enforcement Scenarios and Responses**

  Scenarios::

  – OpenScape Branch and OpenScape SBC prevent licensed features from working if the License Server does not respond to a request for a refresh of licenses for 30 consecutive days (OpenScape Branch or OpenScape SBC has successfully received license information from OpenScape Branch Assistant / OpenScape SBC Assistant at least once). This can happen when there is a communication error or when the licenses are already allocated to another hardware device.

  – If the licenses have been released for a device the OpenScape Branch Assistant / OpenScape SBC Assistant will return zero as the value for all licenses for a device as a response to a license refresh request from a device. In this case licensed features shall be blocked by the device.

  – If the Evaluation license file has expired, the OpenScape Branch Assistant / OpenScape SBC Assistant will return zero as the value for all licenses for a device whenever a license refresh request is sent. In this case licensed features shall be blocked by the device.

  Responses:

  – A pop-up is provided to alert the craft whenever a OpenScape Branch or OpenScape SBC is created but installation data and/or licensing data has not been configured for the device.

  – If no Licenses of any type are available OpenScape Branch or OpenScape SBC will operate normal for 30 days and generate a daily alarm with text indicating how many days before the OpenScape Branch or OpenScape SBC will not provide any calls since no licenses are installed.

License Update

The OpenScape Branch and OpenScape SBC requests licensing update for the following:

- after every reboot
- after changing from survivable mode to normal mode (OpenScape Branch)
- every 24 hours (based on the last reboot time)

License Validation

The OpenScape Branch and OpenScape SBC validate licenses periodically with the central License Server (CMP). If validation fails, additional attempts are made to validate licenses:

- OpenScape Branch/OpenScape SBC to License Server (CMP) Validation:

  The OpenScape Branch/OpenScape SBC checks the License server (CMP) once a day to validate licenses.

  If the first request fails a second attempt is made 30 minutes later, a third attempt 15 minutes after that and an forth attempt 5 minutes later. In other words, 4 tries during the one hour period. After the four validation attempts; validation attempts will take place once every 24 hours.

  – If the connection from the OpenScape Branch/OpenScape SBC to the License server (CMP) is restored within the grace period; the grace period operation returns to normal.
  – If the grace period expires, licensed features stop working. Periodic checking from the OpenScape Branch/OpenScape SBC to the License server (CMP) continues. If the connection to the License server is restored after the grace period expires, operation returns to normal.
- The Network must be fixed to allow communication between the OpenScape Branch and the License server (CMP) for centralized license operation. Stand-alone licensing can be used at the OpenScape Branch/OpenScape SBC to bring operation back to normal (Notice: The OpenScape Branch/OpenScape SBC must be configured for Stand Alone license operation).
- Number of Users in the OpenScape Branch Exceeds the Number of Allowed Registered Users: If the number of users in the OpenScape Branch exceeds the number of allowed registered users, additional registrations are allowed. The number of additional registrations dependant on the OpenScape Branch type.

6.12.5 License Security

This Common Management Platform (CMP), OpenScape Branch and OpenScape SBC secures licensing information in the following ways:

Securing Licensing in the OpenScape Branch and OpenScape SBC

- Licensing information stored in the OpenScape Branch and OpenScape SBC is secured by encryption.
- The OpenScape Branch and OpenScape SBC automatically sets the Branch or SBC licensing to secure mode if it is in unsecured mode and the Licensing Information request contains a correct authentication statement. This function is performed regardless of whether the licenses are configured
- Authentication Statements are encrypted and saved in the backup and . The Authentication Statements are usable after restore.

Securing Licensing in the OpenScape Branch and OpenScape SBC Assistant

- Licensing information stored in the OpenScape Branch Assistant and OpenScape SBC Assistant is secured by encryption. Secured information includes the Logical-IDs, MAC addresses, Authentication Statements and License counts
- The OpenScape Branch Assistant and OpenScape SBC Assistant only allow Authentication Statement requests in unsecured mode. License Information requests are not possible in unsecured mode

- Authentication Statements are included in the backup and are available after restore. The Authentication Statements encrypted and persist over restarts and upgrades.

Index

mitel.com

© 2025 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.