



Configuring SBC and LYNC in TLS Environment

In this section:

- Global Configuration
- Configuration in the Lync Side (Enterprise Network)
- Configuration in the Service Provider Side (SP Network)
- Global Call Routing Configuration

Use this example procedure to configure the SBC and Lync server to use TLS/SRTP.

 This page provides sample configuration; therefore, the values provided will vary based on the user environment.

 The pathCheck Profile on Lync IP-Peer needs to be disabled while switching from TCP to TLS and vice versa.

 **Note**
The SBC 52x0 and SBC 7000 systems support creating IP Interface Groups containing sets of IP interfaces that are not "processor friendly" (i.e. carried on physical Ethernet ports served by separate processors). However, restrictions exist regarding the usage of such Interface Groups.

(This ability does not apply to the SBC 51x0 and SBC 5400 systems which have only two physical media ports. IP interfaces from the two physical ports may be configured within the same IP Interface Groups without restriction.)

For complete details, refer to [Configuring IP Interface Groups and Interfaces](#).

 **Note**
[Sonus recommends using the highest TLS version supported by both the SBC and the peer equipment.](#)

Global Configuration

This section provides the global configuration.

1. Create Codec Entry.
 - a. Create G.711 Codec Entry or create G.711 with Silence Suppression Codec Entry for Comfort Noise.

```
set profiles media codecEntry G711_2833_20 dtmf relay rfc2833
set profiles media codecEntry G711_2833_20 packetSize 20
```

OR

```
set profiles media codecEntry G711SS_2833_20 sendSid enable dtmf relay rfc2833
set profiles media codecEntry G711SS_2833_20 packetSize 20
```

2. Set RTCP interval.


```
set system media mediaRtcpControl senderReportInterval 5
```

3. Create SIP Domains for Mediation Servers to be used with Call Transfer.

```
set global sipDomain med1.domain.com  
set global sipDomain med2.domain.com
```

4. Configuring Tone And Announcement Profile.

```
set profiles media toneAndAnnouncementProfile LRBT_PROF  
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone  
signalingTonePackageState enable makeInbandToneAvailable enable  
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone flags  
useThisLrbtForIngress enable  
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone flags dynamicLRBT  
enable  
set system mediaProfile compression 75 tone 25
```

 The System Media Profile configuration applies to hardware platforms (5000 series, 5400, 7000) only.


5. Create a configuration object to hold a locally generated RSA key pair.

```
set system security pki certificate SBC_CERT type local-internal
```

6. Generate Key pair and CSR (certificate signing request) for submission to a Certificate Authority (CA).

```
request system security pki certificate SBC_CERT generateCSR csrSub  
/C=US/ST=MA/L=Westford/O=Sonus/CN=sbc.domain.com keySize keySize1K
```

7. Generate the required certificates.

 Follow certification generation procedure at [Managing Certificates](#), and then copy the Lync Server Root Certificate (`rootcert.cer`) and Microsoft signed SBC Certificate (`servercert.pem`) into `/opt/sonus/external/` folder of SBC.

8. Create Crypto Suite Profile.

```
set profiles security cryptoSuiteProfile CRYPT_PROF entry 1 cryptoSuite  
AES-CM-128-HMAC-SHA1-80
```

9. Import Lync Root Certificate into database.

```
set system security pki certificate LYNC_CERT type remote fileName rootcert.cer state enabled
```

10. Import Microsoft Certified SBC Server Certificate into database.

```
set system security pki certificate SBC_CERT fileName servercert.pem state enabled
```

11. Create TLS Profile.

```
set profiles security tlsProfile TLS_PROF clientCertName SBC_CERT serverCertName SBC_CERT  
cipherSuite1 rsa-with-aes-256-cbc-sha cipherSuite2 rsa-with-aes-128-cbc-sha authClient true  
allowedRoles clientandserver acceptableCertValidationErrors invalidPurpose
```

Configuration in the Lync Side (Enterprise Network)

The following configuration is required in the Lync side:

1. Create Path Check Profile.

```
set profiles services pathCheckProfile LYNC_OPTIONS protocol sipOptions sendInterval 20  
replyTimeoutCount 1 recoveryCount 1
```

2. Create Packet Service Profile with G.711 or create Packet Service Profile with G.711 w/ Silence Suppression.

```
# Using G.711 Codec  
set profiles media packetServiceProfile LYNC_PSP  
set profiles media packetServiceProfile LYNC_PSP codec codecEntry1 G711_2833_20  
set profiles media packetServiceProfile LYNC_PSP rtcpOptions rtcp enable  
terminationForPassthrough enable  
set profiles media packetServiceProfile LYNC_PSP preferredRtpPayloadTypeForDtmfRelay 101  
set profiles media packetServiceProfile LYNC_PSP silenceInsertionDescriptor  
g711SidRtpPayloadType 13 heartbeat enable  
# Using G.711 Codec with Silence Suppression for Comfort Noise  
set profiles media packetServiceProfile LYNC_PSP  
set profiles media packetServiceProfile LYNC_PSP codec codecEntry1 G711SS_2833_20  
set profiles media packetServiceProfile LYNC_PSP rtcpOptions rtcp enable  
terminationForPassthrough enable  
set profiles media packetServiceProfile LYNC_PSP preferredRtpPayloadTypeForDtmfRelay 101  
set profiles media packetServiceProfile LYNC_PSP silenceInsertionDescriptor  
g711SidRtpPayloadType 13 heartbeat enable  
set profiles media packetServiceProfile LYNC_PSP packetToPacketControl transcode only  
set profiles media packetServiceProfile LYNC_PSP packetToPacketControl  
codecsAllowedForTranscoding thisLeg g711u otherLeg g711u
```

3. Configure Packet Service Profile with Crypto Suite.

```

set profiles media packetServiceProfile LYNC_PSP secureRtpRtcp cryptoSuiteProfile CRYPT_PROF
set profiles media packetServiceProfile LYNC_PSP secureRtpRtcp flags enableSrtp enable
set profiles media packetServiceProfile LYNC_PSP secureRtpRtcp flags allowFallback disable
### IF MEDIA BYPASS ENABLED
set profiles media packetServiceProfile LYNC_PSP secureRtpRtcp flags resetROConKeyChange
disable
set profiles media packetServiceProfile LYNC_PSP secureRtpRtcp flags
resetEncDecROConDecKeyChange enable
### IF MEDIA BYPASS DISABLED
set profiles media packetServiceProfile LYNC_PSP secureRtpRtcp flags resetROConKeyChange
enable
set profiles media packetServiceProfile LYNC_PSP secureRtpRtcp flags
resetEncDecROConDecKeyChange disable

```

4. Create IP Signaling Profile.

```

set profiles signaling ipSignalingProfile LYNC_IPSP
set profiles signaling ipSignalingProfile LYNC_IPSP commonIpAttributes flags
includeReasonHeader enable
set profiles signaling ipSignalingProfile LYNC_IPSP commonIpAttributes flags sendPtimeInSdp
enable
set profiles signaling ipSignalingProfile LYNC_IPSP commonIpAttributes flags
sendRtcpPortInSdp enable
set profiles signaling ipSignalingProfile LYNC_IPSP commonIpAttributes
optionTagInRequireHeader suppressReplaceTag enable
set profiles signaling ipSignalingProfile LYNC_IPSP commonIpAttributes flags
routeUsingRecvFqdn enable
set profiles signaling ipSignalingProfile LYNC_IPSP commonIpAttributes flags
publishIPInHoldSDP enable
set profiles signaling ipSignalingProfile LYNC_IPSP commonIpAttributes flags
minimizeRelayingOfMediaChangesFromOtherCallLegAll enable
set profiles signaling ipSignalingProfile LYNC_IPSP commonIpAttributes flags
relayDataPathModeChangeFromOtherCallLeg enable
set profiles signaling ipSignalingProfile LYNC_IPSP egressIpAttributes
numberGlobalizationProfile DEFAULT_IP
set profiles signaling ipSignalingProfile LYNC_IPSP egressIpAttributes domainName
useZoneLevelDomainNameInContact enable
set profiles signaling ipSignalingProfile LYNC_IPSP egressIpAttributes transport type1
tlsOverTcp
set profiles signaling ipSignalingProfile LYNC_IPSP ingressIpAttributes flags
sendSdpIn2000kIf18xReliable enable

```

5. Create Feature Control Profile.

```

set profiles featureControlProfile LYNC_FCP ipProtocolFlags useIpProtocol enable
defaultCalledUser enable

```

6. Create IP Interface Group.

```

set addressContext a1 ipInterfaceGroup LIF1 ipInterface PKT0_V4 ceName LYNC_SBC portName pkt0
set addressContext a1 ipInterfaceGroup LIF1 ipInterface PKT0_V4 ipAddress 10.10.10.11 prefix
24
set addressContext a1 ipInterfaceGroup LIF1 ipInterface PKT0_V4 mode inService state enabled

```

7. Create Zone.

```
set addressContext a1 zone LYNC_ZONE id 2
set addressContext a1 zone LYNC_ZONE domainName sbc.domain.com
```

8. Create SIP Signaling Port.

```
set addressContext a1 zone LYNC_ZONE id 2 sipSigPort 2 ipInterfaceGroupName LIF1 ipAddressV4
10.10.10.11 portNumber 5060 tlsProfileName TLS_PROF transportProtocolsAllowed sip-tls-tcp
state enabled mode inService
```

9. Create External DNS Group or local DNS group.

```
# Configuring External DNS Group
set addressContext a1 dnsGroup EXT_DNS
set addressContext a1 dnsGroup EXT_DNS type mgmt server DNS1 ipAddress 10.10.10.10 state
enabled
set addressContext a1 zone LYNC_ZONE dnsGroup EXT_DNS

# Configuring Local DNS Group
set addressContext a1 dnsGroup LOCAL_DNS
set addressContext a1 dnsGroup LOCAL_DNS localRecord DNS1 hostName lync.domain.com data 1
ipAddress 10.10.10.22 state enabled
set addressContext a1 dnsGroup LOCAL_DNS localRecord DNS1 hostName lync.domain.com data 2
ipAddress 10.10.10.23 state enabled
set addressContext a1 dnsGroup LOCAL_DNS localRecord DNS1 hostName lync.domain.com order
roundrobin state enabled
set addressContext a1 dnsGroup LOCAL_DNS localRecord DNS1 state enabled

set addressContext a1 dnsGroup LOCAL_DNS localRecord DNS2 state enabled hostName
med1.domain.com data 1 ipAddress 10.10.10.22 state enabled
set addressContext a1 dnsGroup LOCAL_DNS localRecord DNS3 state enabled hostName
med2.domain.com data 1 ipAddress 10.10.10.23 state enabled
```



You can configure centralized round-robin or strict round-robin for first-come first-served basis. Centralized round-robin is not recommended for high call traffic volume.

For distributed round-robin over a large volume of traffic, configure the following:

```
set addressContext a1 dnsGroup LOCAL_DNS localRecord DNS1 hostName lync.domain.com order
roundrobin state enabled
```

10. Create SIP Trunk.

```

set addressContext a1 zone LYNC_ZONE sipTrunkGroup LYNC_TG media mediaIpInterfaceGroupName
LIF1
set addressContext a1 zone LYNC_ZONE sipTrunkGroup LYNC_TG policy media packetServiceProfile
LYNC_PSP
set addressContext a1 zone LYNC_ZONE sipTrunkGroup LYNC_TG policy signaling
ipSignalingProfile LYNC_IPSP
set addressContext a1 zone LYNC_ZONE sipTrunkGroup LYNC_TG downstreamForkingSupport enabled
set addressContext a1 zone LYNC_ZONE sipTrunkGroup LYNC_TG signaling rel100Support enabled
set addressContext a1 zone LYNC_ZONE sipTrunkGroup LYNC_TG signaling acceptHistoryInfo
enabled
set addressContext a1 zone LYNC_ZONE sipTrunkGroup LYNC_TG services dnsSupportType a-only
set addressContext a1 zone LYNC_ZONE sipTrunkGroup LYNC_TG ingressIpPrefix 10.10.10.0 24
set addressContext a1 zone LYNC_ZONE sipTrunkGroup LYNC_TG policy featureControlProfile
LYNC_FCP
set addressContext a1 zone LYNC_ZONE sipTrunkGroup LYNC_TG mode inService state enabled

```

11. Configure IP Peer for LYNC listening on port 5067 for TLS:

```

set addressContext a1 zone LYNC_ZONE ipPeer LYNC_IPP
set addressContext a1 zone LYNC_ZONE ipPeer LYNC_IPP policy sip fqdn lync.domain.com fqdnPort
5066
set addressContext a1 zone LYNC_ZONE ipPeer LYNC_IPP pathCheck profile LYNC_OPTIONS hostName
lync.domain.com hostPort 5066 state enabled

```



The SBC will listen for TLS session initiation on the configured port number + 1. So if the SIP signaling port is configured for port 5066, the SBC will listen for TLS on port 5067. The SBC does not allow direct control over the port number used for TLS, but other devices do. It is important to communicate the correct port for SIP/TLS to the peers so that they will correctly configure the TCP port number used for TLS.

12. Create Static Route.

```

set addressContext a1 staticRoute 10.10.10.22 32 10.10.10.1 LIF1 PKT0_V4 preference 100

```



If you are using IPv6 addressing, then Static Route, IP Peer and Ingress IP Prefix needs to be configured as per IPv6 addressing scheme.

Here is an example of IP interface group and SIP signaling port configuration in the Lync Side using IPv6 addressing scheme:

```

###Create IP Interface Group
set addressContext a1 ipInterfaceGroup LIF1 ipInterface PKT0_V4 altIpAddress fc00::10:f:f:f:11
altPrefix 64

###Create SIP Signaling Port
set addressContext a1 zone LYNC_ZONE id 2 sipSigPort 2 ipAddressV6 fc00::10:f:f:f:11

```

Configuration in the Service Provider Side (SP Network)

There is no specific parameters to be set on Service Provider side hence standard trunkgroup creation procedure needs to be followed based on deployment. The below provides example configuration.



To play LRBT, apply 'Tones and Announcement' profile on trunkgroup as appropriate.

1. Create Packet Service Profile.

```
set profiles media packetServiceProfile SP_PSP
set profiles media packetServiceProfile SP_PSP codec codecEntry1 G711_2833_20
set profiles media packetServiceProfile SP_PSP rtcpOptions rtcp enable
set profiles media packetServiceProfile SP_PSP preferredRtpPayloadTypeForDtmfRelay 101
set profiles media packetServiceProfile SP_PSP silenceInsertionDescriptor
g711SidRtpPayloadType 13 heartbeat enable
```

2. Create IP Signaling Profile.

```
set profiles signaling ipSignalingProfile SP_IPSP
set profiles signaling ipSignalingProfile SP_IPSP commonIpAttributes flags
includeReasonHeader enable
set profiles signaling ipSignalingProfile SP_IPSP commonIpAttributes flags sendPtimeInSdp
enable
set profiles signaling ipSignalingProfile SP_IPSP commonIpAttributes flags sendRtcpPortInSdp
enable
set profiles signaling ipSignalingProfile SP_IPSP egressIpAttributes flags
disable2806Compliance enable
set profiles signaling ipSignalingProfile SP_IPSP ingressIpAttributes flags
sendSdpIn2000kIf18xReliable enable
```

3. Create IP Interface Group.

```
set addressContext a1 ipInterfaceGroup LIF2 ipInterface PKT1_V4 ceName LYNCSCB portName pkt1
set addressContext a1 ipInterfaceGroup LIF2 ipInterface PKT1_V4 ipAddress 20.20.20.11 prefix
24
set addressContext a1 ipInterfaceGroup LIF2 ipInterface PKT1_V4 mode inService state enabled
```

4. Create Zone.

```
set addressContext a1 zone SP_ZONE id 3
```

5. Create SIP Signaling Port.

```
set addressContext a1 zone SP_ZONE id 3 sipSigPort 3 ipInterfaceGroupName LIF2 ipAddressV4
20.20.20.11 portNumber 5060 transportProtocolsAllowed sip-tcp,sip-udp state enabled mode
inService
```

6. Create SIP Trunk.

```
set addressContext a1 zone SP_ZONE sipTrunkGroup SP_TG media mediaIpInterfaceGroupName LIF2
set addressContext a1 zone SP_ZONE sipTrunkGroup SP_TG policy media packetServiceProfile
SP_PSP
set addressContext a1 zone SP_ZONE sipTrunkGroup SP_TG policy media
toneAndAnnouncementProfile LRBT_PROF
set addressContext a1 zone SP_ZONE sipTrunkGroup SP_TG policy signaling ipSignalingProfile
SP_IPSP
set addressContext a1 zone SP_ZONE sipTrunkGroup SP_TG ingressIpPrefix 20.20.20.0 24
set addressContext a1 zone SP_ZONE sipTrunkGroup SP_TG mode inService state enabled
```

7. Create IP Peer.

```
set addressContext a1 zone SP_ZONE ipPeer SP_IPP
set addressContext a1 zone SP_ZONE ipPeer SP_IPP ipAddress 20.20.20.22 ipPort 5060
```

8. Create Static Route.

```
set addressContext a1 staticRoute 20.20.20.22 32 20.20.20.1 LIF2 PKT1_V4 preference 100
```

Global Call Routing Configuration

The following is the global call routing configuration:

1. Create Routing Labels.

```
set global callRouting routingLabel LYNC_RL routingLabelRoute 1 trunkGroup LYNC_TG ipPeer
LYNC_IPP inService inService
set global callRouting routingLabel SP_RL routingLabelRoute 1 trunkGroup SP_TG ipPeer SP_IPP
inService inService
```

2. Create Routes.

```
set global callRouting route none Sonus_NULL Sonus_NULL standard 10 1 all all ALL none
Sonus_NULL routingLabel LYNC_RL
set global callRouting route none Sonus_NULL Sonus_NULL standard 20 1 all all ALL none
Sonus_NULL routingLabel SP_RL
set global callRouting route none Sonus_NULL Sonus_NULL username Sonus_NULL Sonus_NULL all
all ALL none med1.domain.com routingLabel LYNC_RL
set global callRouting route none Sonus_NULL Sonus_NULL username Sonus_NULL Sonus_NULL all
all ALL none med2.domain.com routingLabel LYNC_RL
```