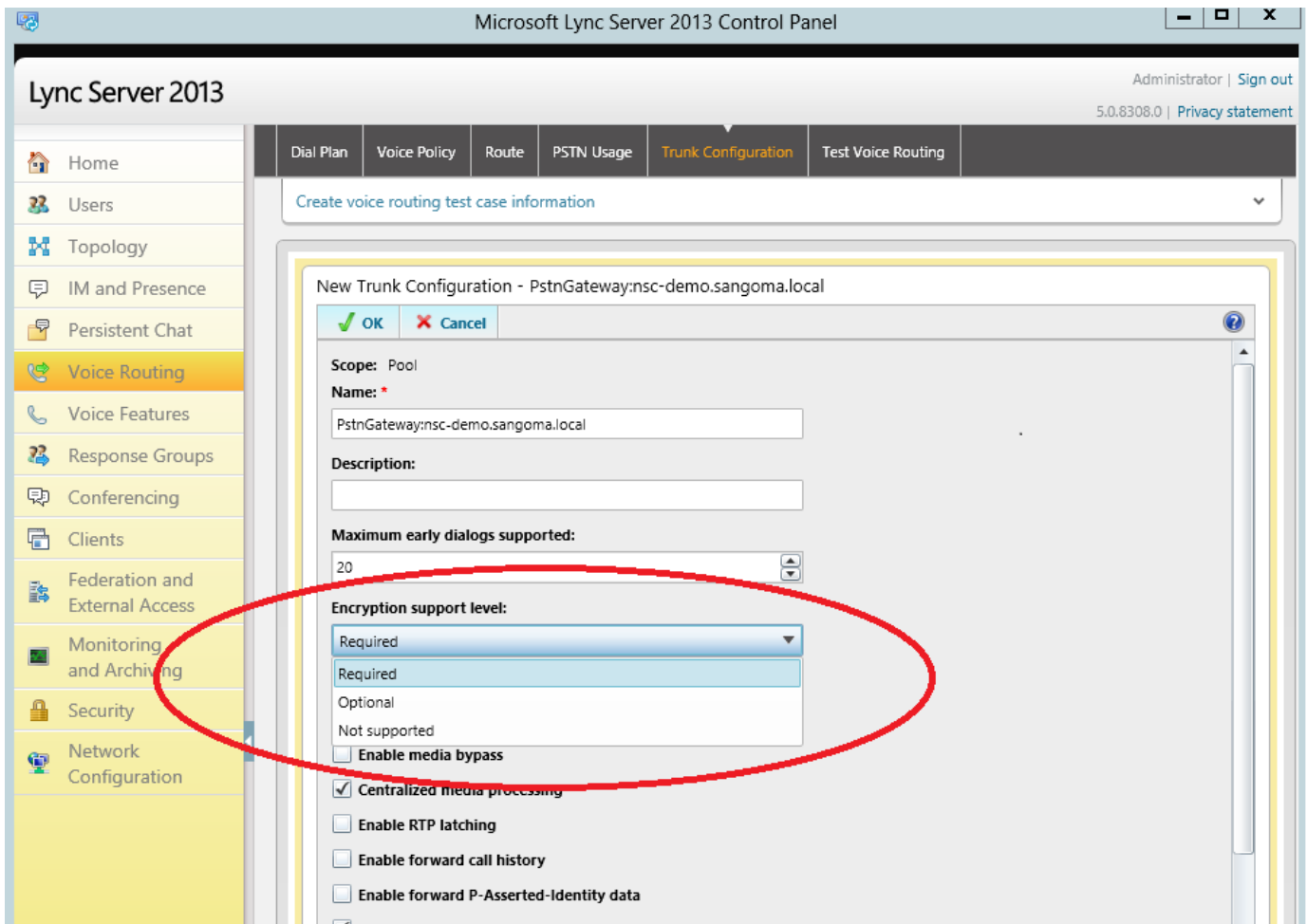


Microsoft Lync 2013 Integration

1. Pre-requirements

Before you start to configure NSC to connect with Lync Server, you need to know some information first:

- a. **Transport type** to use for SIP signalling (TCP or TLS. Lync Mediation Server doesn't support UDP for SIP signalling);
- b. Lync Server **Mediation Server** SIP listening **port** (By default, 5067 for TLS or 5068 for TCP);
- c. **NSC** SIP listening **port**, e.g. I use port 5081 here for either TCP or TLS;
- d. Lync Server Trunk Configuration "**Encryption support level**": Required, Optional or Not Supported



- e. **FQDN** or **IP address** of Lync Server Mediation Server

2. Media Profile

Because Lync only supports G711 codecs (**PCMU** and **PCMA**), it is suggested that you create a media profile that only includes PCMU and PCMA.

- Go to "**Configuration -> Media -> Media Profiles**", create a new media profile named "LyncOnly" (of course you can use other name you like);
- Make sure that only "**PCMU 20ms, PT=0**" and "**PCMA 20ms, PT=8**" are selected;
- Set "**Enable Silence Suppression**" to "Enabled";
- Save the media profile.

Configuration > Media > **Media Profiles**

This page allows managing media profiles. ● System stopped. ● Configuration not completed.

Media profile : LyncOnly

Codec #1	PCMU 20ms, PT=0
Codec #2	PCMA 20ms, PT=8
Codec #3	
Codec #4	
Codec #5	
Codec Negotiation Mode	Prefer-Remote
Enable Silence Suppression	Enable
DTMF Mode	RFC 2833

3. Outbound Call

For a call from Mediation Server to NSC, we call it an outbound call; what we need to do is to create NSC SIP Profile.

- Go to "**Configuration -> Signalling -> SIP Profiles**", add a new sip profile;
- You will have a default configuration, and do the following changes:
 1. "**SIP IP Address**": choose the NIC you want to use for SIP listening;
 2. "**Transport**": choose "TCP" or "TLS" depending on 1-a;
 1. If "Transport" is "TCP", set the value of 1-c (e.g. 5081) into item "**Port**";
 2. if "Transport" is "TLS", set the value of 1-c (5081) to item "**TLS Port**";
 3. note: that when TCP is the only transport, "Port" will be used; if TLS is the only transport, only "TLS Port" is used.
 3. Set both "**Inbound Media Profile**" and "**Outbound Media Profile**" to "LyncOnly"
 4. Set "**Maximum Sip Request URI Length**" to "255"
 5. Set "**Notify REFER on Final Response**" to "Enabled"

6. Set "Lync Interoperability" to "Enabled"
7. Upload TLS Server Certificate in "TLS Certificate"; (check Annex A for more details about Certificate Generation)
8. Set "Authenticate Calls" to "Disabled"
9. Depends on the value of 1-d (Encryption support level):(In real world, if you want a call to be completely secure, please pick TLS and Encryption level "Required")
 1. when it is "Not Supported": "Secure RTP" = "Disabled";
 2. when it is "Required": "Secure RTP" = "Enabled"; "Require Only Secure RTP" = "Enabled"; "Secure AVP" = "Disabled"; "Crypto Life Time" = "Medium"; "Crypto MKI Length" = "1:1";
 3. when it is "Optional": "Secure RTP" = "Enabled"; "Require Only Secure RTP" = "Enabled"; "Secure AVP" = "Enabled"; "Crypto Life Time" = "Medium"; "Crypto MKI Length" = "1:1"

Here below I attach a set of screen shots for TLS configuration:

Overview >

Configuration >

General

- > Core

IP Settings

- > Signaling Interfaces
- > Media Interfaces
- > Routes

Signaling

- > Domains
- > SIP Profiles
- > SIP Trunks
- > RADIUS

Media

- > Media Profiles
- > RTCP Monitor

Routing

- > Call Routing
- > LCR Carriers
- > ENUM
- > Load Balancing

Security

- > IP Firewall
- > SIP Firewall
- > Media Firewall
- > Intrusion Detection
- > CAC Profiles
- > CA Certificates

Reporting

- > CDR
- > SNMP

Management

- > Apply
- > Backup - Restore

System >

Reports >

Help >

Configuration > Signaling > **SIP Profiles**

● System stopped.
● Configuration not completed.

SIP profile : To_Lync_Server

General

User Agent	NetBorder Session Controller
SIP IP Address	eth0 - 10.10.2.64
External SIP IP Address	
Port	5081
Transport	TLS
Outbound Proxy	
RTP IP address	
External RTP IP address	
Inbound Bypass Media	Disable
Inbound Media Profile	LyncOnly
Outbound Media Profile	LyncOnly
SIP Trace	Disable

Interoperability

100 Reliability	Disable
3PCC	Disable
Ignore 183 without SDP	Disable
FQDN in Contact Header	
Maximum Sip Request URI Length	255
Notify REFER on Final Response	Enable
Lync Interoperability	Enable

Timing

SIP Session Timer	Disable
Session Expires	1800
Minimum Session Expires	1800
RTCP Interval	5000

Encryption	
TLS Version	TLS Version 1
TLS Certificate	agent.pem <input type="button" value="Browse..."/>
TLS Passphrase	
Certificate Date Verification	Enable
Certificate Verification Policy	Outgoing
TLS Port	5061
Secure RTP	Enable
Require Only Secure RTP	Enable
Secure AVP	Disable
Crypto Life Time	Medium
Crypto MKI Length	1:1
Authentication	
Authenticate Calls	Disable
Accept Blind Authentication	Disable
Authenticate Requests	Disable
QoS	
SIP TOS Value	
RTP TOS Value	
NAT Traversal	
NAT ACL	-- None --
Ping NAT Registrations	Disable
Symmetric Response Routing	Enable
RTP Auto Adjust	Disable
Aggressive NAT Detection	Disable
Load Limits	
Enable Load Limiting	Enable
Max Concurrent Sessions	
CPU High Threshold	90
CPU Low Threshold	80
Reject Response Code	503
Reject Message	Service Unavailable
Load Limits	
Enable Load Limiting	Enable
Max Concurrent Sessions	
CPU High Threshold	90
CPU Low Threshold	80
Reject Response Code	503
Reject Message	Service Unavailable

Don't forget to link this sip profile to the correct dial plan.

4. Inbound Call

For a call from NSC to Mediation Server, we call it an inbound call; besides the sip profile we defined in section 3, we need to create a new sip trunk

- Go to **"Configuration -> Signalling -> SIP Trunks"**, add a new sip trunk;
- Get the value of 1-e(Mediation Server IP or FQDN) and 1-b(Mediation Server port), create <ip>:<port> format string, e.g. "lync-demo.sangoma.local:5067", and then fill into **"Domain"**;
- Fill in **"User Name"** and **"Password"** with dummy string, like "notuse" and "notuse";
- Fill in **"Transport"** with the value from 1-a;
- **"Options Ping Frequency"** = "60";
- **"Options Max Ping"** = "5";
- **"Options Min Ping"** = "1";
- In Sip Profile, choose the sip profile created in section 3;
- Keep **"Registration"** to "Disabled"
- Save the sip trunk configuration.

Overview

- Configuration
- General
 - Core
- IP Settings
 - Signaling Interfaces
 - Media Interfaces
 - Routes
- Signaling
 - Domains
 - SIP Profiles
 - SIP Trunks**
 - RADIUS
- Media
 - Media Profiles
 - RTCP Monitor
- Routing
 - Call Routing
 - LCR Carriers
 - ENUM
 - Load Balancing
- Security
 - IP Firewall
 - SIP Firewall
 - Media Firewall
 - Intrusion Detection
 - CAC Profiles
 - CA Certificates
- Reporting
 - CDR
 - SNMP
- Management
 - Apply
 - Backup - Restore
- System
- Reports
- Help

Configuration > Signaling > SIP Trunks

This page allows managing SIP Trunk settings.

System stopped.
Configuration not completed.

SIP Trunk : To_Lync_SIP_Trunk

General

Domain	lync-demo.sangoma.local:5067
User Name	notuse
Password	*****
From User	
From Domain	
Transparent CallerID	Enabled
Proxy Address	
Outbound Proxy Address	
Transport	TLS
Contact Host	
Contact Parameters	
OPTIONS Ping Frequency	60
OPTIONS Max Ping	5
OPTIONS Min Ping	1
SIP Profile	To_Lync_Server
Inbound Media Profile	-- SIP Profile Default --
Outbound Media Profile	-- SIP Profile Default --
Routing Plan	-- SIP Profile Default --

Registration

Registration	Disable
Registrar Proxy Address	
Register To: Header	From User
Register Expire Seconds	3600
Register Retry Seconds	30
Register Timeout Seconds	60

Annex A. Certificates for TLS

To make NSC work with Lync Server Mediation Server through TLS, you need to have 2 certificates in hand: CA Root Certificate and Server Certificate.

Get CA Root Certificate from whoever can access your CA authority, rename the extension of the file to ".pem" and then you can upload it into NSC "**CA Certificates**".

For TLS Server Certificate, you need to prepare 2 files: one is your private key (never give file to others); the other is Certificate Request.

A.1 Generation of Certificate Request

To generate a certificate request SSH into the SBC and run the command below. The FQDN being used here is "testsbc.sangoma.com".

```
cd /usr/local/nsc/conf/ssl/  
/usr/local/nsc/bin/gentls_cert create_server_req -cn testsbc.sangoma.com -alt DNS:testsbc.sangoma.com -org sangoma.com  
cat myreq.req
```

At this point your certificate request will be displayed on the SSH window. Copy and paste the text to your CA to generate the certificate.

A.2 Uploading Certificate to SBC.

NSC only supports BASE 64 format, we don't support DER format.

WINS CP into the SBC and copy the certificate file from your CA into /usr/local/nsc/conf/ssl/. Ensure this file is in the Base64 format. As well ensure the file is renamed to "certificate.pem". Once this is done run the commands below to create the agent.pem file. This will contain both the certificate and the private key.

```
cd /usr/local/nsc/conf/ssl/  
cat certificate.pem myreq.key > agent.pem
```

At this point WINS CP the agent.pem to your local desktop and log into the SBC via the webUI and go to Configuration -> Security -> Certificates. Upload the agent.pem as a Server certificate.