Connecting NEC UNIVERGE® SV9100 with Microsoft® Teams Direct Routing Enterprise Model using NEC BX Series SBC

Version History

Version	Date	Notes and Changes
1.0	30/03/2020	1. Initial draft of SV9100 integration document
1.1	09/04/2020	1. Reviewed screenshot of SIP Interfaces
1.2	31/01/2022	1. Updated call scenarios and updated number manipulation rules
1.3	18/02/2022	1. Updated classification rules

Contents

Purpose of this document:

This document is intended as a quick start guide for NEC's UNIVERGE® SV9100 integration with NEC BX series SBCs and Microsoft Teams. Functionality is provided using the Direct Routing feature of the BX Series SBC. Prior knowledge of IP networking and how to connect to a network will be necessary in order to understand the configuration examples and to be able to modify the examples contained in this document.

Knowledge of DNS and TLS Certificates is also required.

Scope of this document

This document demonstrates how to configure an NEC BX Series SBC connecting to Microsoft Teams and SV9100 SIP Tie Line. This guide assumes that the existing network already has separate VLANs for voice and data services.

This document covers configuration of the SV9100 using PCPro Programming tool and NEC BX Using the Web GUI.

The versions tested in this document are;

SV9100 CP20 Main Software 10.50.50
SV9100 CP20 PC Pro 10.30.51
NEC BX9000 7.20A.254.565

Integration is limited to voice dialling only. Video calls are not supported over Direct Routing trunks, BLF or presence information is not shared.

Prerequisites:

The following prerequisites are necessary in order to achieve MS Teams integration using Direct Routing.

Microsoft Office 365 Subscription

Microsoft Teams and Direct Routing are only offered through these Enterprise plans;

- E1 (Plan 2), E3 (Plan 2), or E5 (Plan 1 or 2)

**E5 has 2 license Plans where Apps and Add-Ons are excluded (Plan 1) or included (Plan 2)

Apps, and Add-Ons needed to enable Teams Direct Routing:

- Microsoft 365 Audio Conferencing (optional for conference feature)
- Microsoft 365 Phone System (Formerly Skype for Business (SfB))

NEC BX SBC licensing

The minimum requirements for the BX SBC are;

- SBC Sessions – For calls traversing the SBC, one session is required for each concurrent call
- BX MS Teams license – Required for connection to MS Teams. This is a global license
- Transcoding licenses* – Optional, recommended. Required for use of SILK NB and WB codecs

* Without transcoding capability G.711 codec will be used.

UNIVERGE® SV9100

MS Teams connection utilises the SIP trunking capability of the SV9100. For each SIP trunk the following is required;

- IP Trunk license (BE114065) – One license is required for each concurrent call
- System Capacity license (BEBE114042) – Required for additional system capacity

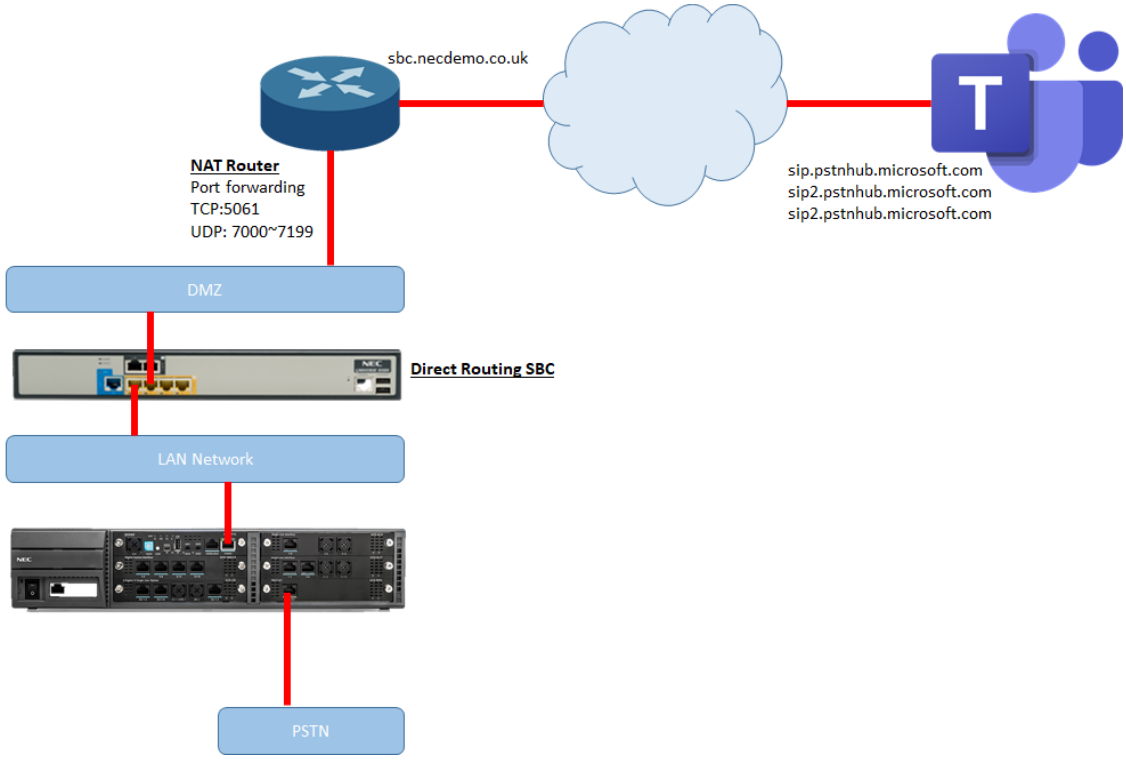
Network Infrastructure

The connection to MS Teams Cloud PBX is ***only*** supported using TLS. This means the following networking requirements must be met.

- Fixed public IP Address for WAN connection
- FQDN (Fully Qualified Domain Name) for the SBC
- DNS Entry for the SBC (for example sbc.customer.com) – See connectivity diagram
- Public trusted certificate for the SBC (See this link for trusted CAs https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc)
- Firewall configuration supporting port forwarding for SIP connectivity – See connectivity diagram
- DNS Server to resolve FQDN of MS Teams Cloud PBX service

Test Network

In the test network the SBC has two interfaces, one in the DMZ and one in the LAN. The PSTN is connected to the SV9100 and the MS Teams users are allowed to dial through the SV9100. It is also possible to connect the PSTN trunks to the SBC if a SIP carrier is used, or the hardware gateway.



Public DNS records have been created to resolve sbc.necdemo.co.uk to the public IP address of the customer router. The customer router then forwards connections from port TCP:5061 to the SBC.

General BX SBC Configuration

General configuration of the SBC is outside the scope of this document, for further detail please see integration whitepapers and training materials.

TLS Configuration

TLS is a mandatory requirement for connection with MS Teams.

If you already have a TLS certificate issued for this host/domain then it can be loaded directly into the SBC. Otherwise it is necessary to create a CSR (Certificate Signing Request) which is then issued by the CA (Certificate Authority). If you are purchasing a new TLS Security Certificate please check that the issuer is trusted by Microsoft (https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc)

Creating a CSR can be done from the *IP NETWORK > SECURITY > TLS Contexts* menu. For further information on creating the CSR please see the BX User Manuals.

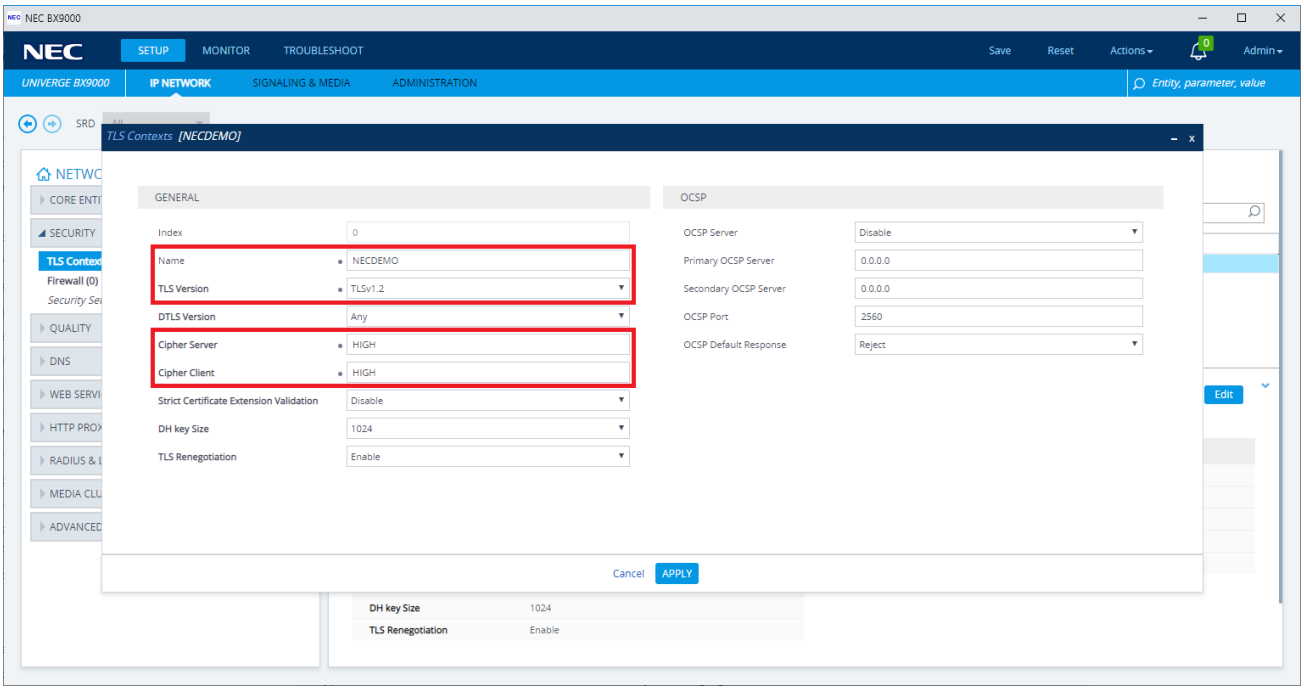
Configure your TLS Context

To load your TLS Security Certificate into the BX;

1. Log into the web interface of the BX (for example https://192.168.88.5)
2. Navigate to *IP NETWORK > SECURITY > TLS Contexts*
3. Either modify the existing TLS Context (0*) or add a new TLS Context

*If you modify TLS context 0 this Security Certificate will also be used to secure the programming Web GUI of the SBC.

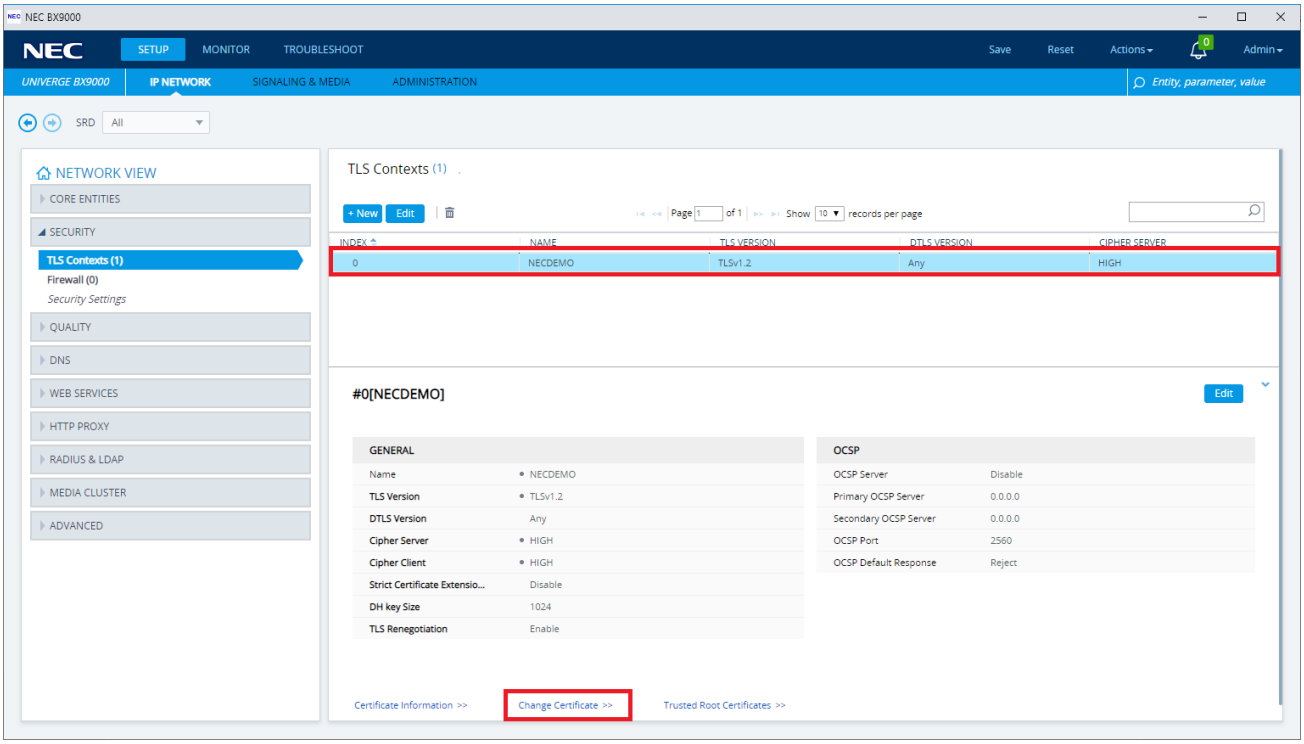
In the screenshot below the default TLS context has been renamed to 'NECDEMO', replace this name with your customer name, ensure that only TLSv1.2 is enabled and for further security restrict the supported Ciphers to HIGH only.



Deploy the Certificates and Private Key

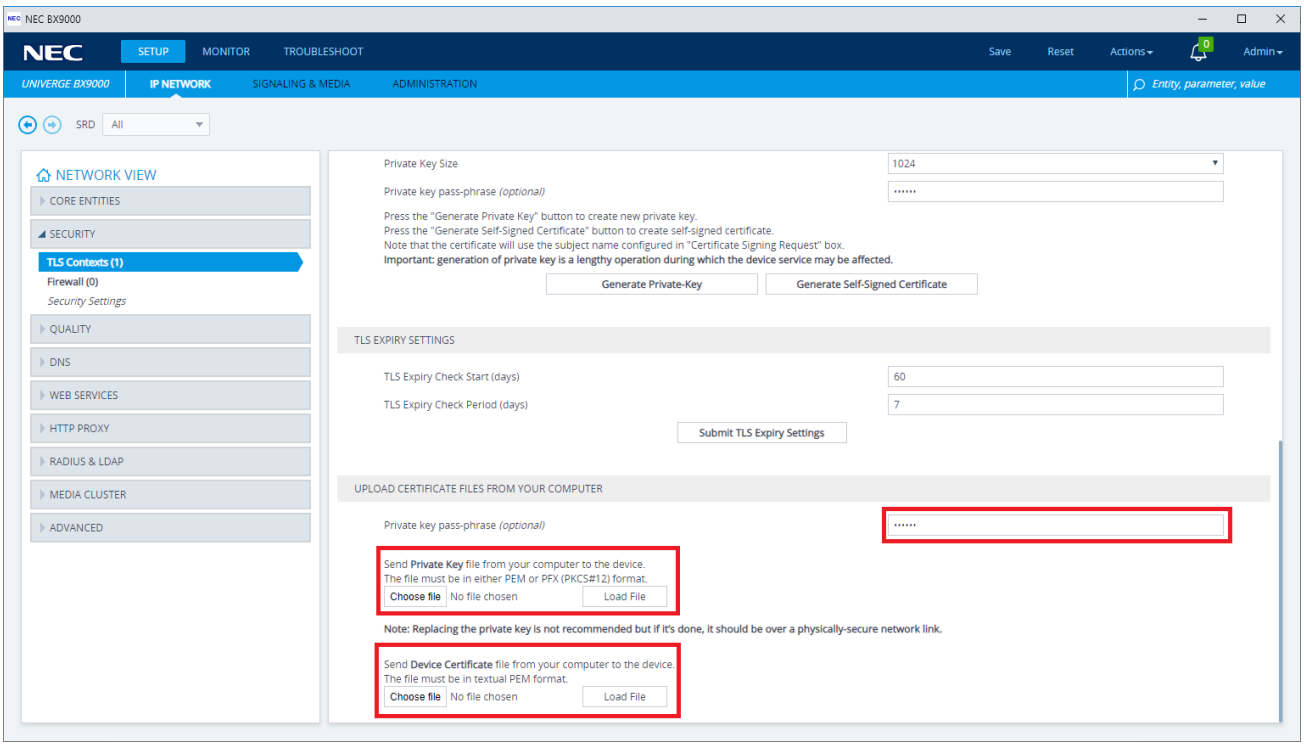
In the SBC Web GUI return to the TLS Contexts page and do the following;

1. Select the required TLS Context index row (named NECDEMO) and then select the *Charge Certificate* link located at the bottom of the detail pane.

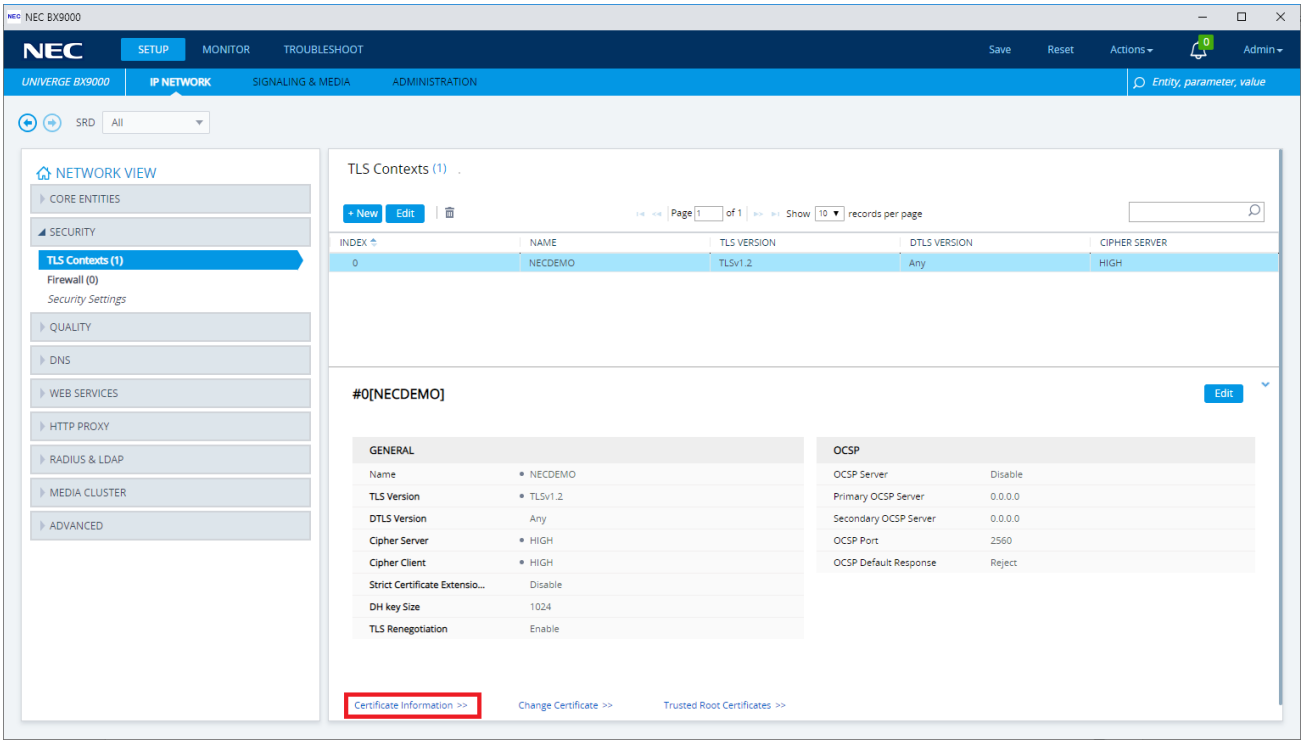


2. Scroll down to the *UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER* group and upload your Private Key file and Device Certificate files*. If the Private Keu file is encrypted then enter the password in the pass-phrase box. When you upload the files you will see a verification if successful.

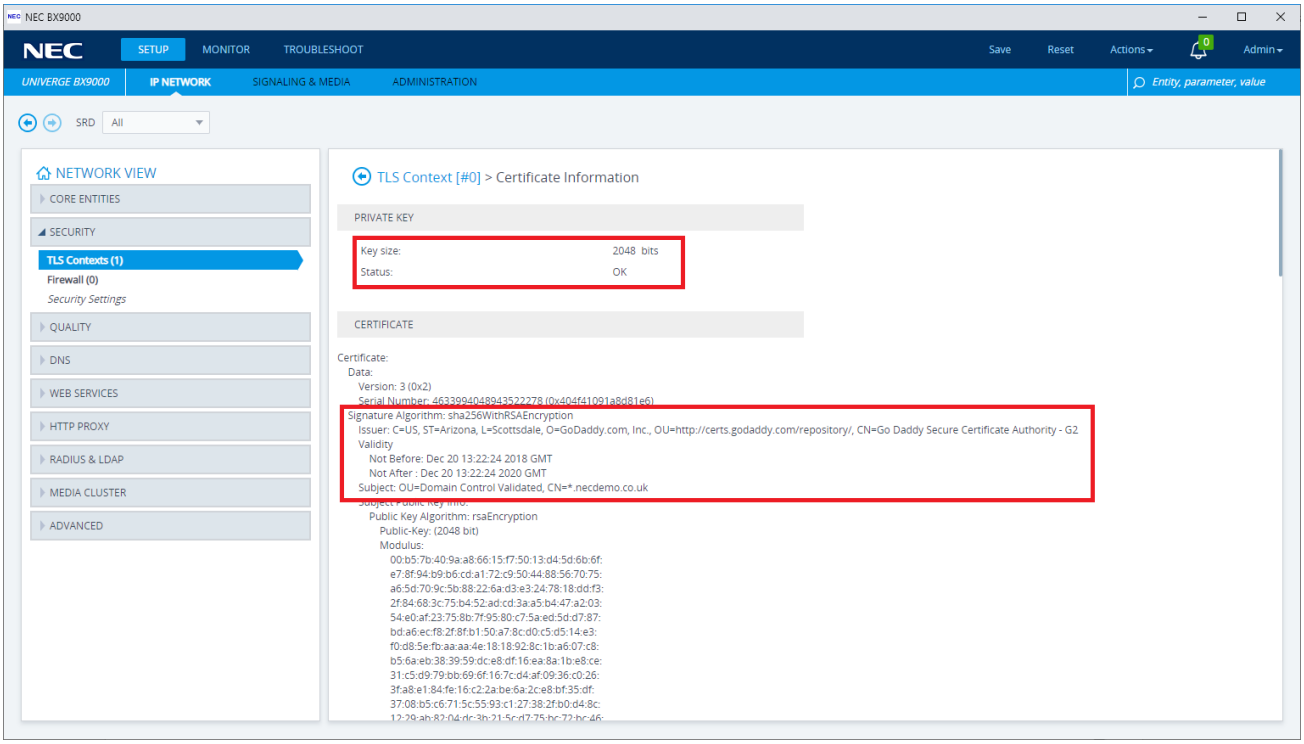
* The uploaded certificate files should be PEM encoded with .pem, .cer or .crt file extension.



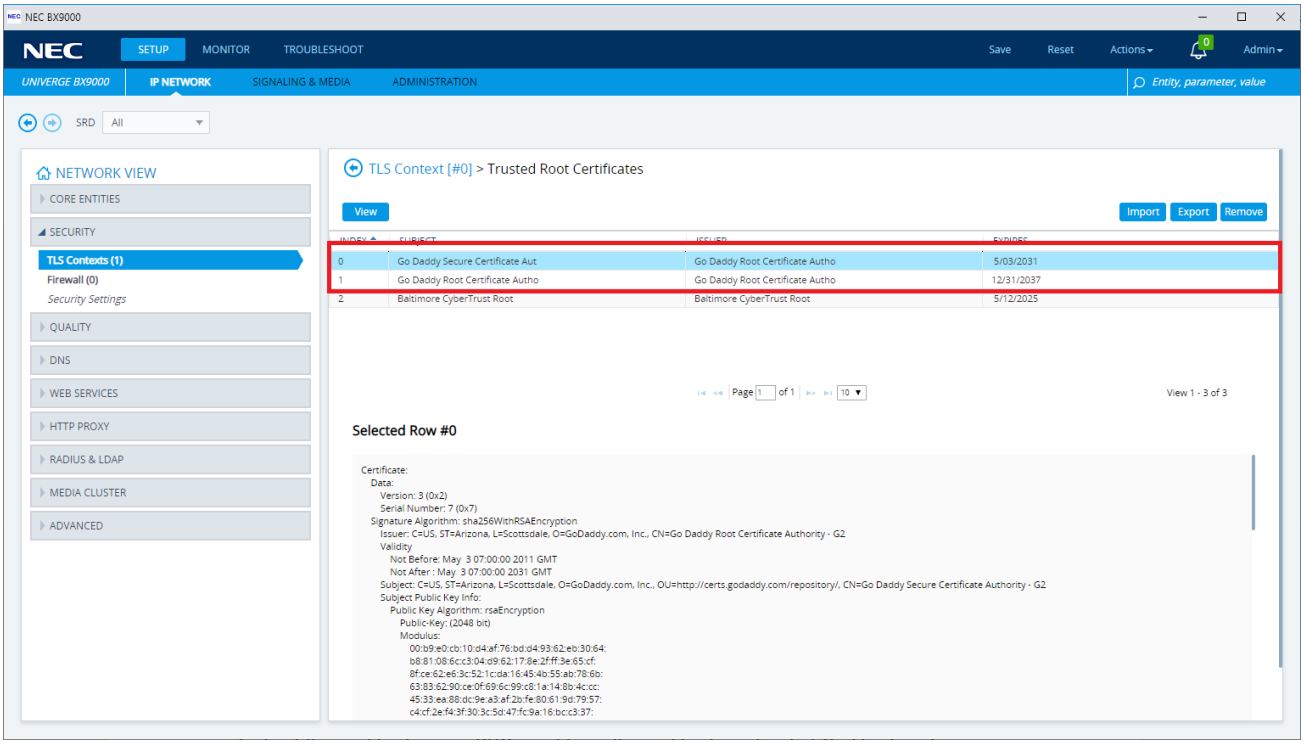
3. Validate that the certificate and private key were uploaded correctly. From the TLS Contexts page, choose the *Certificate Information* link to see detail about the uploaded certificate.



4. If the Status is OK then you can continue to the next steps, otherwise go back and check the uploaded files.



5. Upload the root and any intermediate certificates to the *Trusted Root Certificate* store. These are provided as part of the certificate bundle by the issuer and can be found in the issuer's online repository. In this example the certificate chain is part of the Go Daddy Secure Certificate Authority - G2 chain.



Deploy Baltimore Trusted Root Certificate

Note: Loading Baltimore Trusted Root Certificates to is mandatory for implementing an MTLS connection with the Microsoft Teams network.

The DNS name of the Teams Direct Routing interface is **sip.pstnhub.microsoft.com**. In this interface, a certificate is presented which is signed by Baltimore Cyber Baltimore CyberTrust Root with Serial Number: 02 00 00 b9 and SHA fingerprint: d4:de:20:d0:5e:66:fc:53:fe:1a:50:88:2c:78:db:28:52:ca:e4:74.

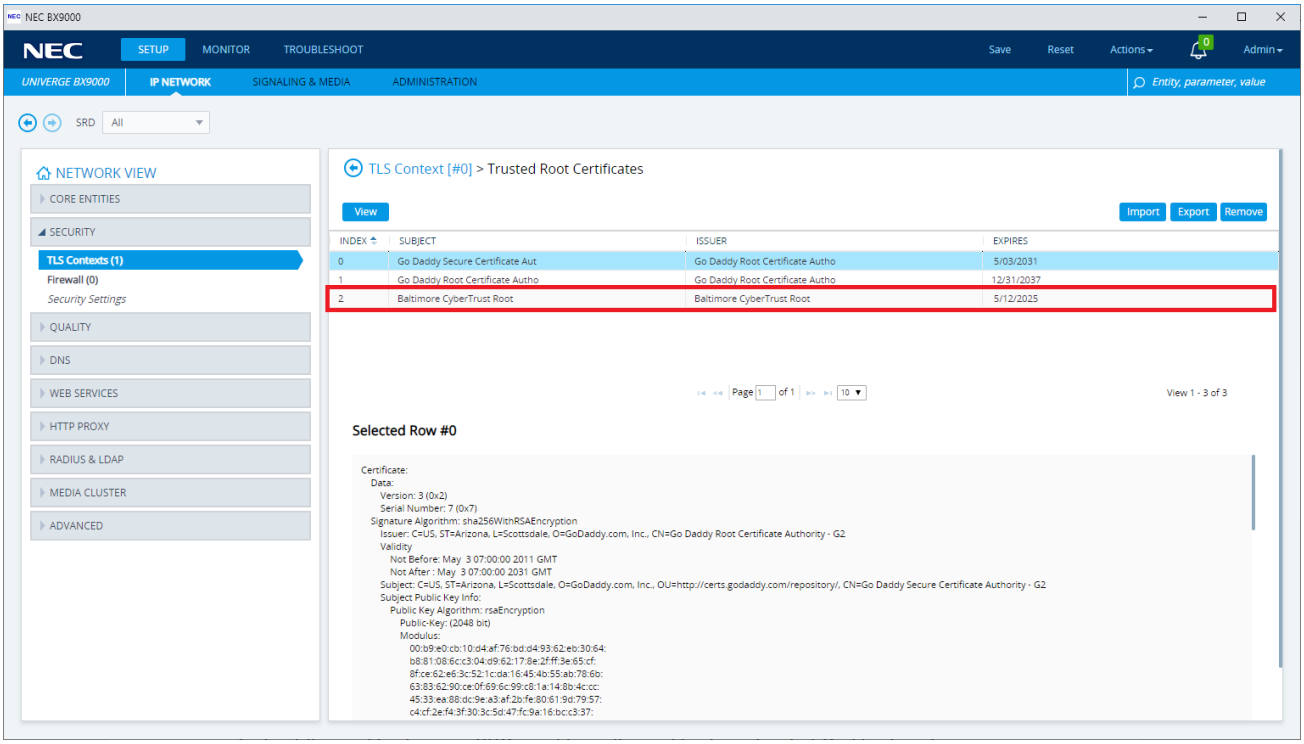
To trust this certificate, your SBC *must* have the certificate in Trusted Certificates storage. Download the certificate from https://cacert.omniroot.com/bc2025.pem and follow the steps above to import the certificate to the Trusted Root storage.

Note: Before importing the Baltimore root certificate into the SBC, make sure it's in .PEM or .PFX format. If it isn't, you need to convert it to .PEM or .PFX format, otherwise the 'Failed to load new certificate' error message is displayed. To convert to PEM format, use Windows local store on any Windows OS and then export it as 'Base-64 encoded X.509 (.CER) certificate'.

Download the Baltimore Trusted Root certificate from the online repository here;

https://cacert.omniroot.com/bc2025.pem

Upload the certificate to the *Trusted Root Certificate* store.



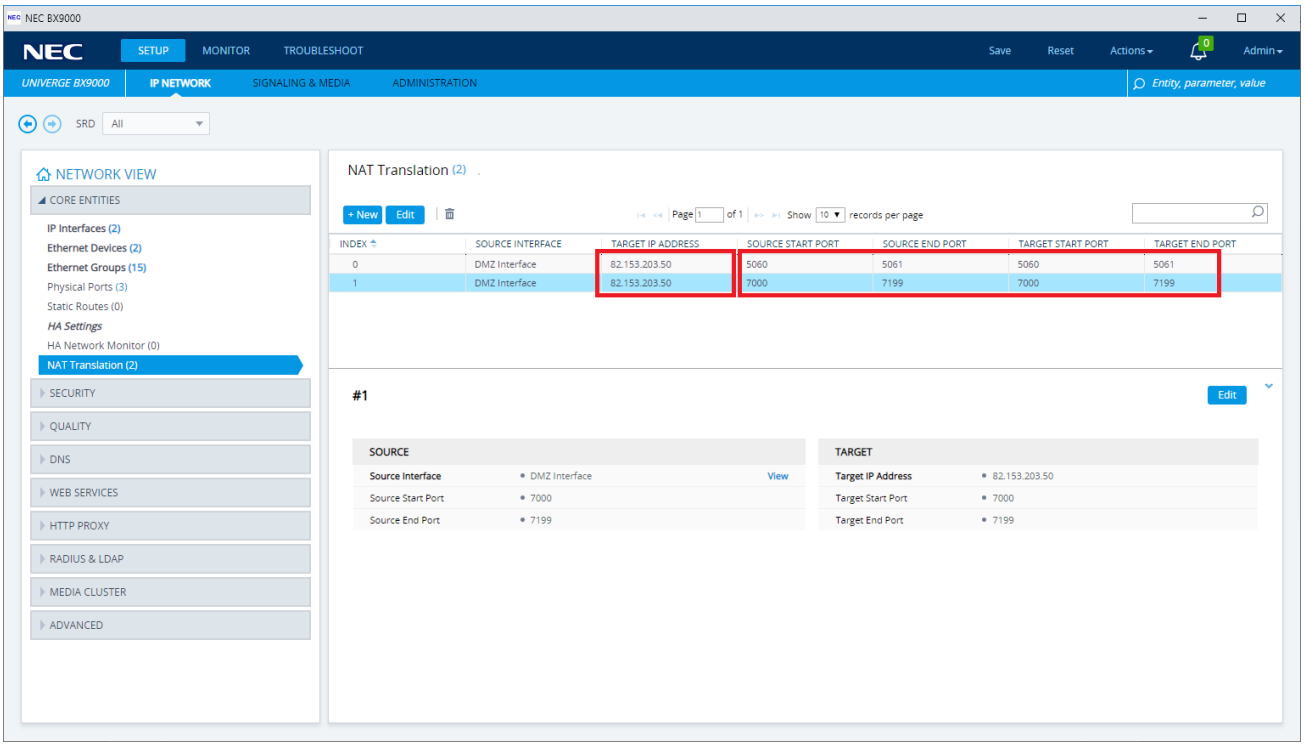
Configure IP Interfaces and NAT Traversal

In this example the SBC has one leg in the LAN and one leg in the DMZ network. The customer router is configured to forward the following ports to the DMZ interface of the SBC.

TLS Signalling – TCP:5061
RTP Media – UDP:7000~7199

For further information on IP Interface setup refer to the NEC BX SBC Training Material and the BX User Manuals.

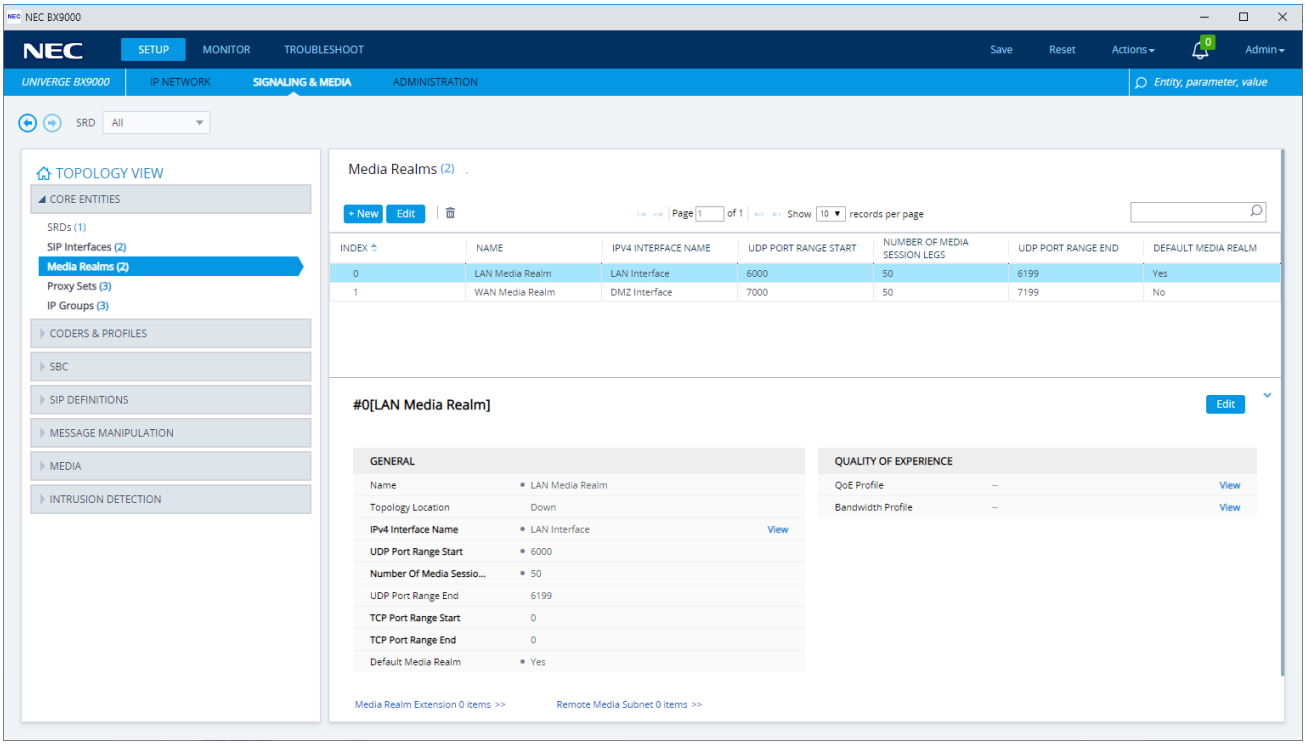
NAT Translation if configured to ensure that SIP Signalling includes the Public IP address of the customer site instead of the internal private IP address.

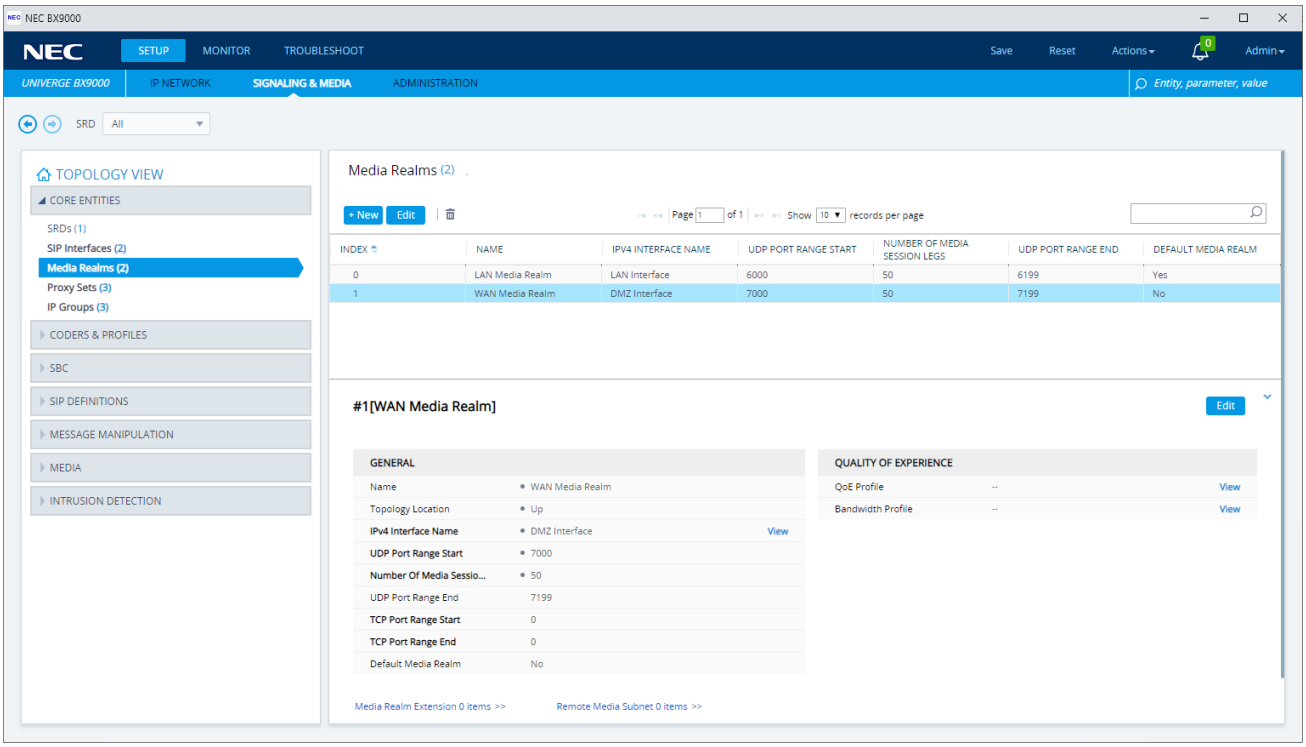


Configure Media Realms

Media Realms define the UDP ports used to terminate and generate RTP media on the device. Media Realms are defined in *SETUP > SIGNALING & MEDIA > CORE ENTITIES> Media Realms*. In the example below two Media Realms are defined;

LAN Media Realm – This is bound to the LAN IP Interface and occupies UDP ports 6000~6199
WAN Media Realm – This is bound to the WAN IP Interface and occupies UDP ports 7000~7199





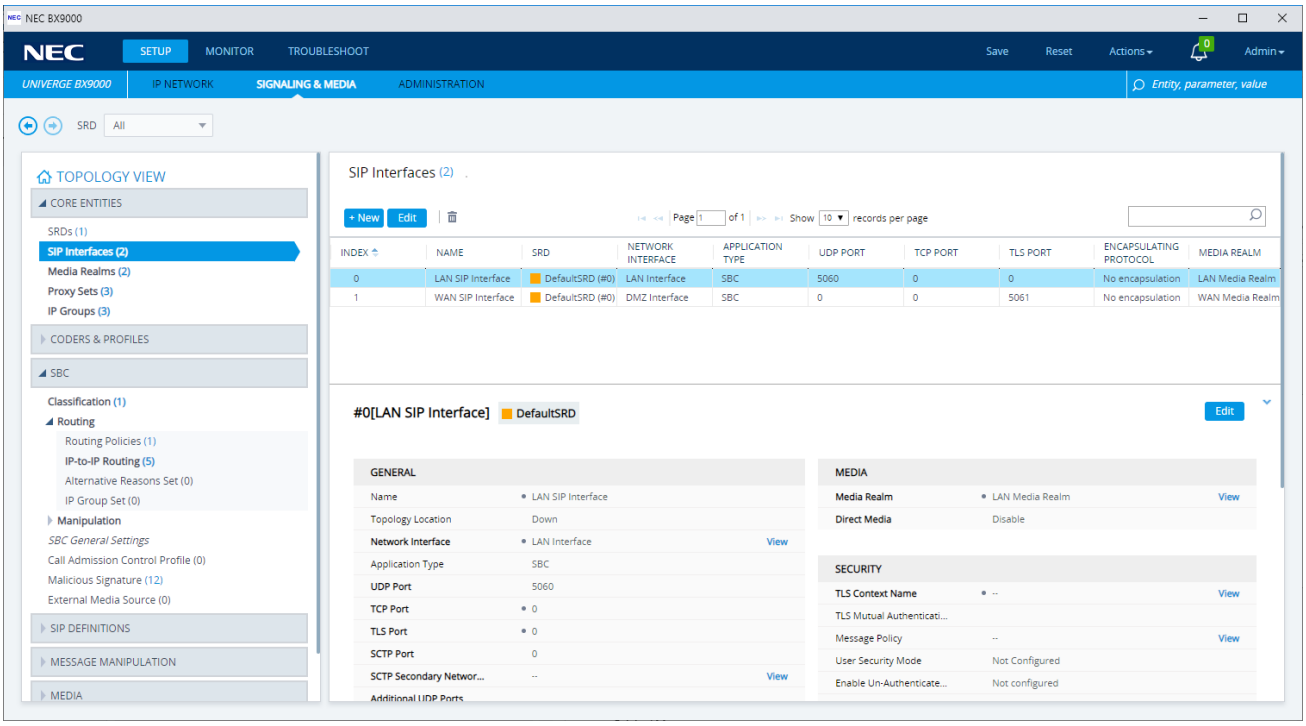
Configure SIP Interfaces

This section shows how to configure the SIP listening interfaces for the SBC. SIP communication between the SBC and MS Teams only supports TLS transport. Please note the configuration below is only an example and may change if you have connections to other services such as SIP Carriers or Branch Offices using the same interface.

It is good practise to disable any transports which are not being used. SIP Interfaces are configured under *SETUP > SIGNALING & MEDIA > CORE ENTITIES > SIP Interfaces*.

Note: The Direct Routing interface can only use TLS for a SIP port. It does not support using TCP due to security reasons. The SIP port might be any port of your choice. When pairing the SBC with Office 365, the chosen port is specified in the pairing command.

The LAN SIP Interface is used to terminate SIP signalling between the SBC and SV9100 PBX.
The WAN SIP Interface is used to terminate SIP signalling between the SBC and MS Teams Cloud PBX.



Note: For implementing an MTLS connection with the Microsoft Teams network, configure 'TLS Mutual Authentication' to "Enable" for the Teams SIP Interface.

Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response	Media Realm	TLS Context Name	TLS Mutual Authentication
LAN SIP Interface	LAN Interface	SBC	5060	0	0	Disable	500	LAN Media Realm	-	-
WAN SIP Interface	WAN Interface	SBC	0	0	5061	Enable	0	WAN Media Realm	NECDEMO	-

* **Note!** Loading the Baltimore Trusted Root Certificate is mandatory for implementing MLTS connection.

Configure Proxy Sets and Proxy Addresses

The Proxy set defines a service connected to the SBC, the parameters, ports hostnames or IP addresses which are used to communicate with this service.

Microsoft Cloud PBX provides three redundant FQDNs for resiliency.

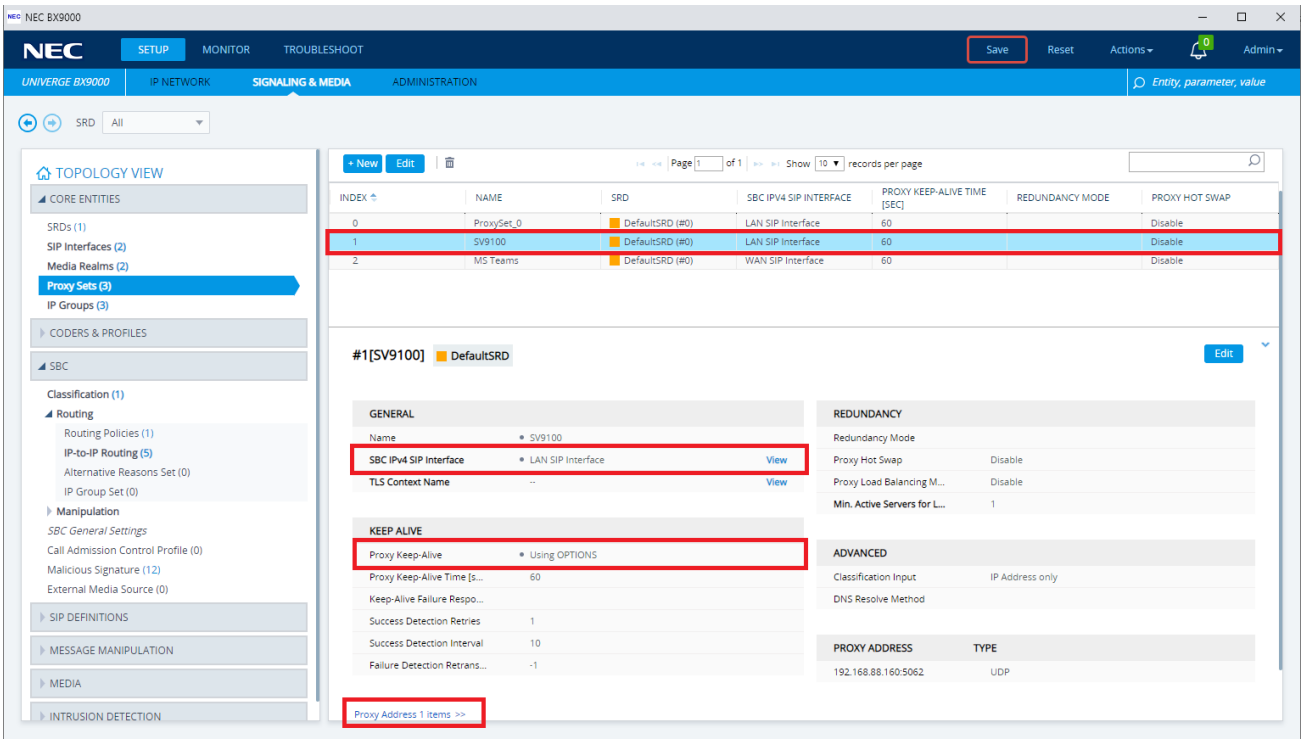
- sip.pstnhub.microsoft.com – Global FQDN – must be tried first. When the SBC sends a request to resolve this name, the Microsoft Azure DNS servers return an IP address pointing to the primary Azure datacentre assigned to the SBC. The assignment is based on performance metrics of the datacentres and geographical proximity to the SBC. The IP address returned corresponds to the primary FQDN.
- sip2.pstnhub.microsoft.com – Secondary FQDN – geographically maps to the second priority region.
- sip3.pstnhub.microsoft.com – Tertiary FQDN – geographically maps to the third priority region.

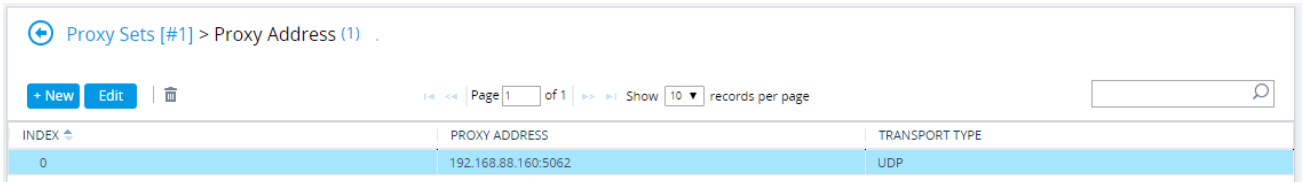
For more information see Microsoft Documentation (https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-fqdns).

To configure the Proxy Sets navigate to *SETUP > SIGNALING & MEDIA > CORE ENTITIES > Proxy Sets*.

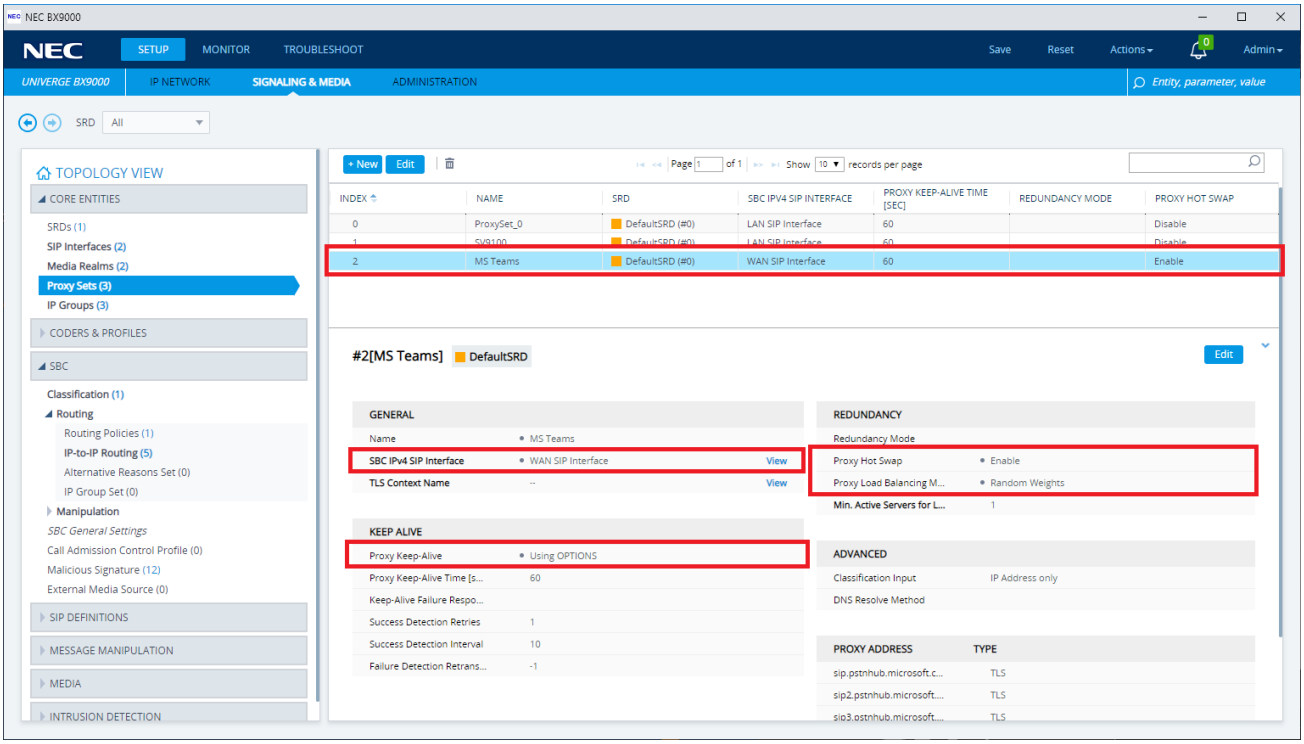
In this example SIP Trunk Profile 2 is used on the SV9100. If Profile 1 is used change the signalling port from 5062 to 5060.

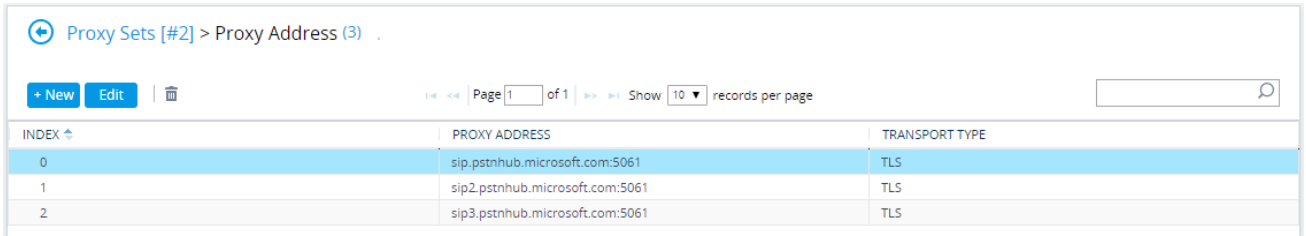
1. Configure a Proxy Set for the SV9100. Ensure that OPTIONS method is selected for the Proxy Keep-Alive method and that the LAN SIP Interface is used. Using the Proxy Address child table (link at bottom of the page) configure the IP:Port of the SV9100.





2. Configure a Proxy Set for MS Teams. Ensure that OPTIONS method is selected for the Proxy Keep-Alive method and that the WAN SIP Interface is used. Using the Proxy Address child table (link at bottom of the page) configure the FQDN addresses for MS Cloud PBX.

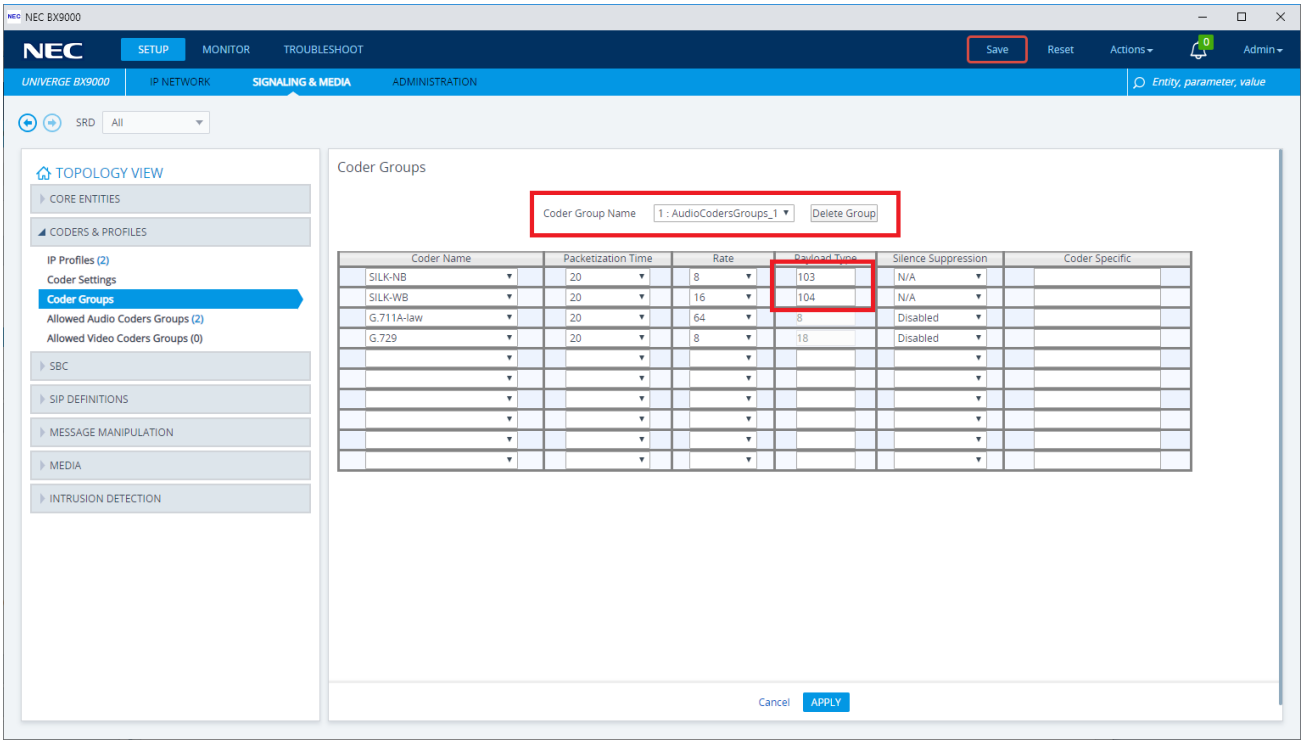




Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	sip.pstnhub.microsoft.com:5061	TLS	1	1
1	sip2.pstnhub.microsoft.com:5061	TLS	2	1
2	sip3.pstnhub.microsoft.com:5061	TLS	3	1

Configure Coder Groups

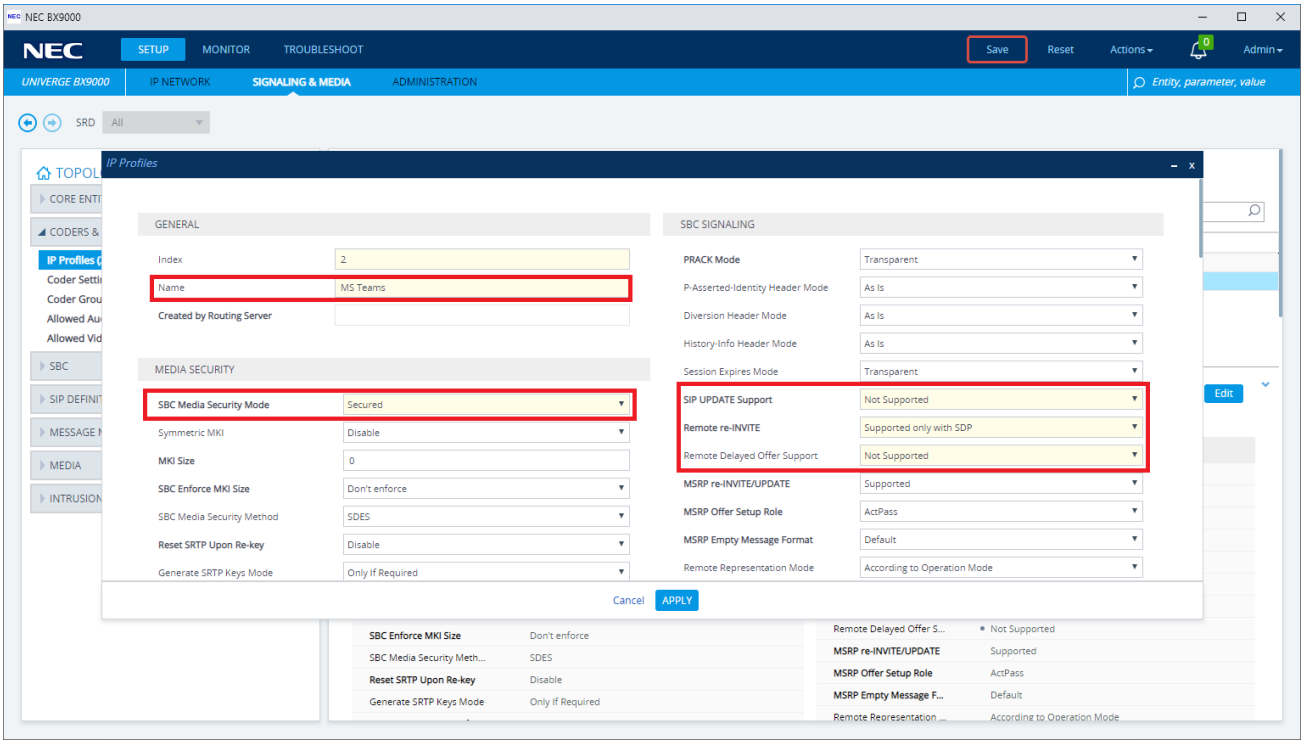
This section describes how to configure coders. Teams Direct Routing supports SILK NB and WB codecs as well as G.711. To create the coder group navigate to *SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Coder Groups*. Enable the codecs which you would like to use towards MS Teams. Transcoding is optional and described later in this document.



Configure the IP Profile for Direct Routing to MS Teams

This section describes how to configure IP Profiles. An IP Profile is a set of parameters with user-defined settings related to signalling (e.g., SIP message terminations such as REFER) and media (e.g., coder type). An IP Profile needs to be assigned to the specific IP Group.

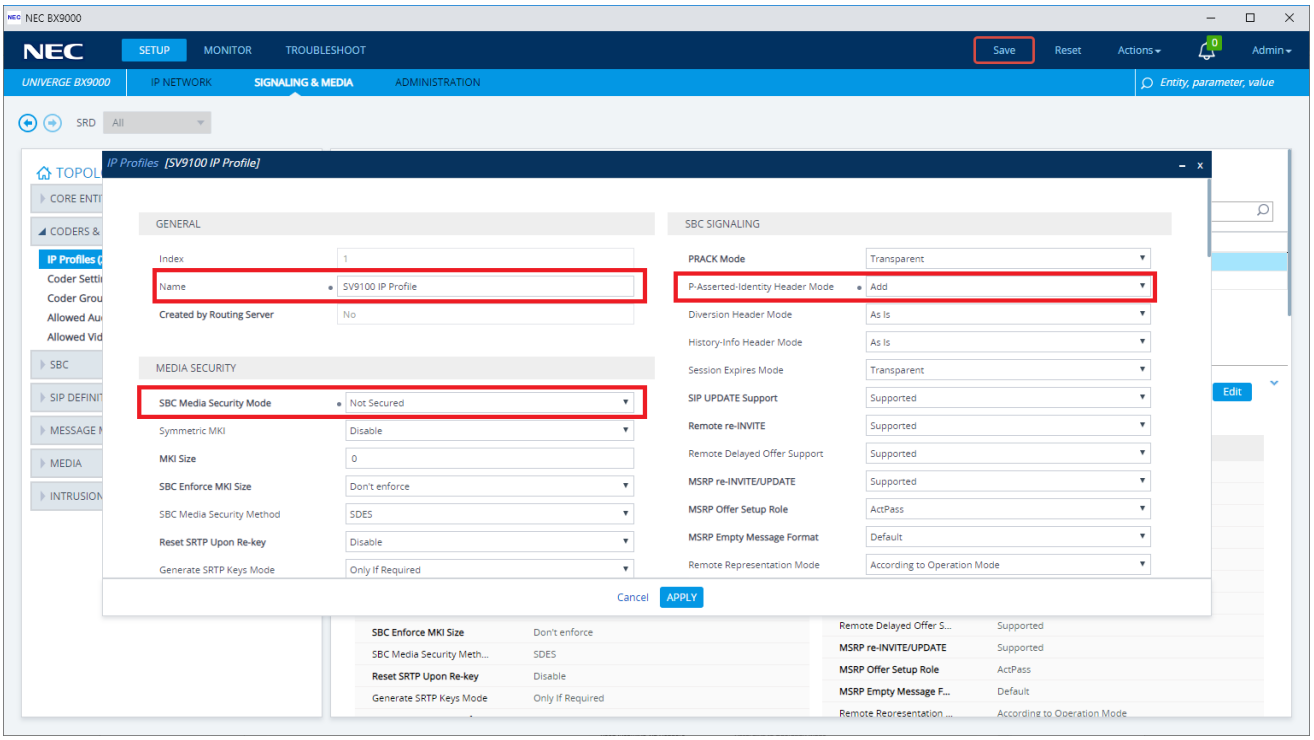
1. Open the IP Profiles table in *SETUP > SIGNALING & MEDIA > CODERS & PROFILES > IP Profiles.* Use the **+New** button to add a new IP Profile.



Name	Parameter
General	
Name	MS Teams IP Profile (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	Secured
SBC Early Media	
Remote Early Media RTP Detection Mode	By Media (required, as Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18X response)
SBC Media	
Extension Coders Group	AudioCodersGroups_1
RTCP Mode	Generate Always (required, as some ITSPs do not send RTCP packets during Hold, but Microsoft expects them)
ICE Mode	Lite (required only when Media Bypass enabled on Teams)
SBC Signaling	
Remote Update Support	Not Supported
Remote re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
SBC Forward and Transfer	
Remote Refer Mode	Handle Locally
Remote Replaces Mode	Handle Locally
Remote 3XX Mode	Handle Locally
SBC Hold	
Remote Hold Format	Inactive (some SIP Trunk may answer with a=inactive and IP=0.0.0.0 in response to the Re-Invite with Hold request from Teams. Microsoft Media Stack doesn't support this format. So, SBC will replace 0.0.0.0 with its IP address)
All other parameters can be left unchanged at their default values.	

Configure the IP Profile for the SV9100

1. Open the IP Profiles table in *SETUP > SIGNALING & MEDIA > CODERS & PROFILES > IP Profiles.* Use the **+New** button to add a new IP Profile.

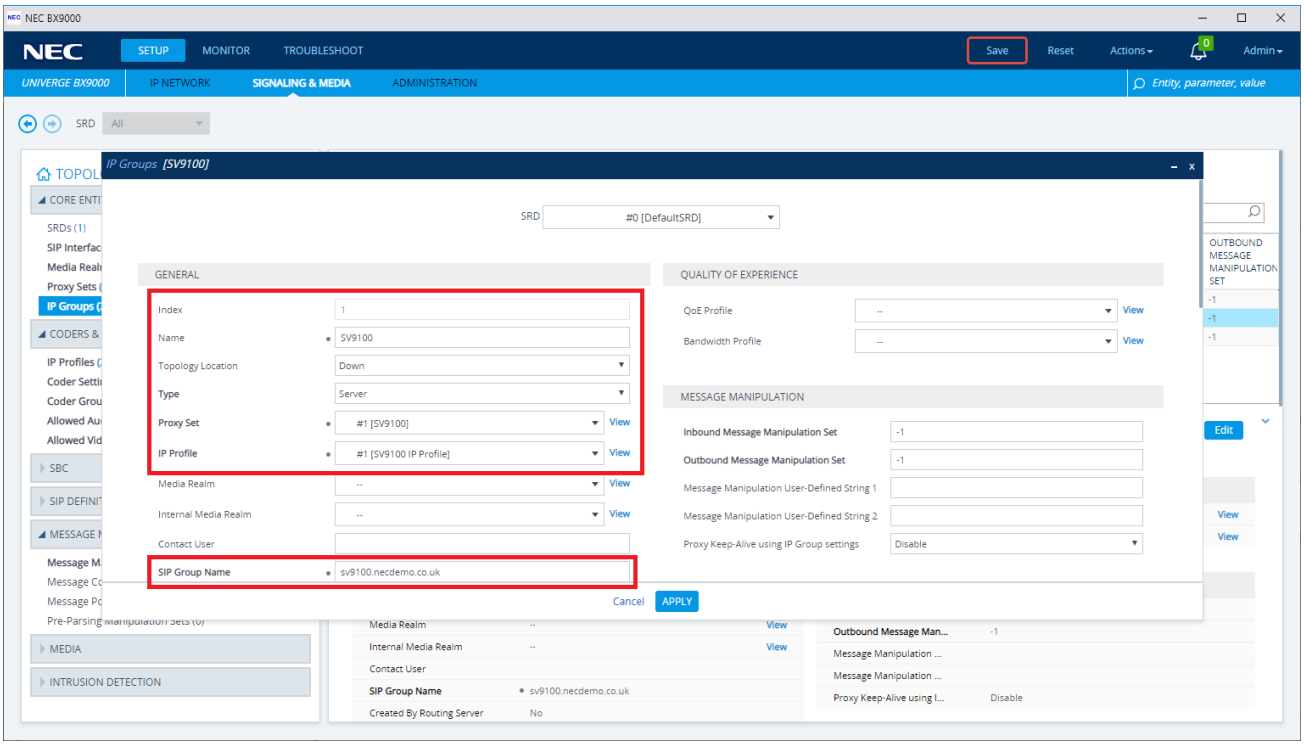


Name	Parameter
General	
Name	SV9100 IP Profile (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	Not Secured
SBC Signaling	
P-Asserted-Identity Mode	Add (required for anonymous calls)
SBC Forward and Transfer	
Remote Refer Mode	Handle Locally
Remote Replaces Mode	Handle Locally
Remote 3XX Mode	Handle Locally
All other parameters can be left unchanged at their default values.	

Configure IP Groups

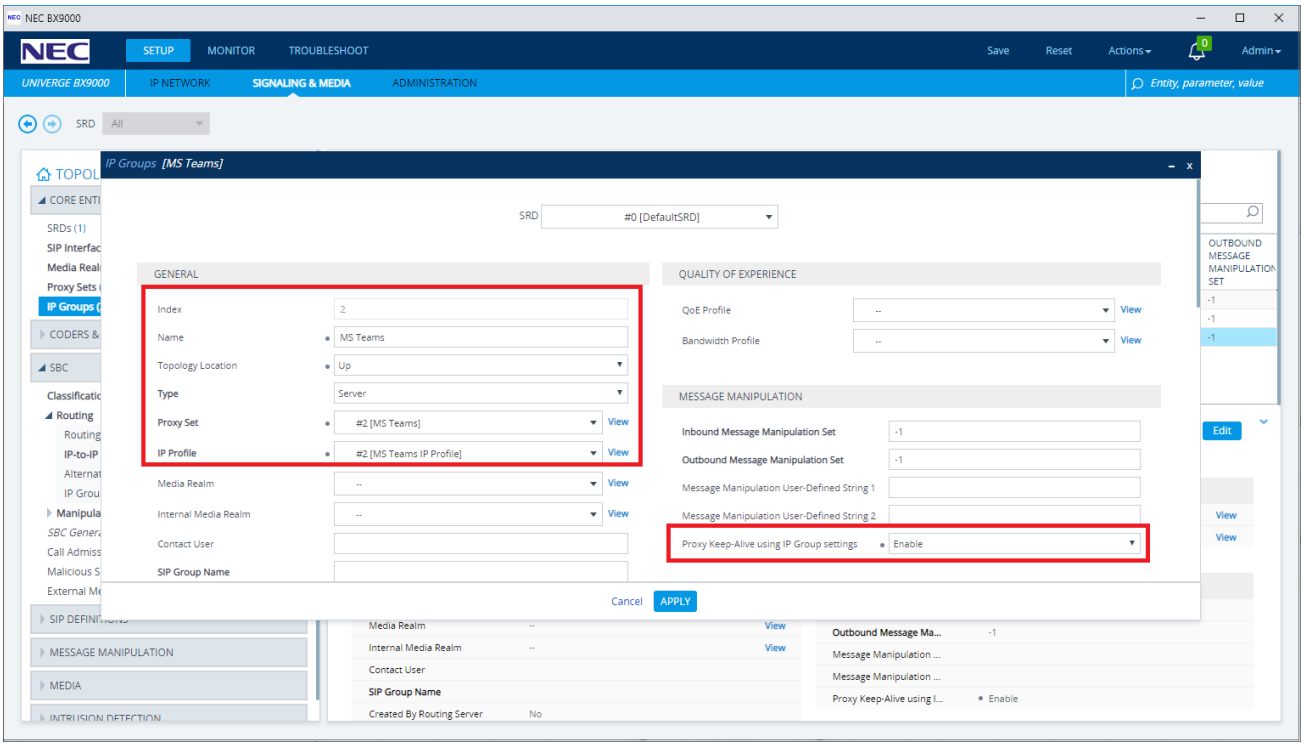
This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP-PBX or SIP Trunk) or it can be a group of users. For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

1. Configure an IP Group for the SV9100. Navigate to *SETUP > SIGNALING & MEDIA > CORE ENTITIES > IP Groups* to create the group. For the SV9100 the IP Group will support a REGISTER from the SV9100.



Name	Parameter
General	
Name	SV9100 (arbitrary descriptive name)
Topology Location	Down
Type	Server
Proxy Set	SV9100
IP Profile	SV9100 IP Profile
SIP Group Name	sv9100.necdemo.co.uk (change as per customer requirements)
SBC General	
Classify By Proxy Set	Enabled
SBC Registration and Authentication	
Authentication Mode	SBC as Server
Authentication Method List	REGISTER
Username	SV9100 (will be set in the SV9100)
Password	Choose a complex password (will be set in the SV9100)
All other parameters can be left unchanged at their default values.	

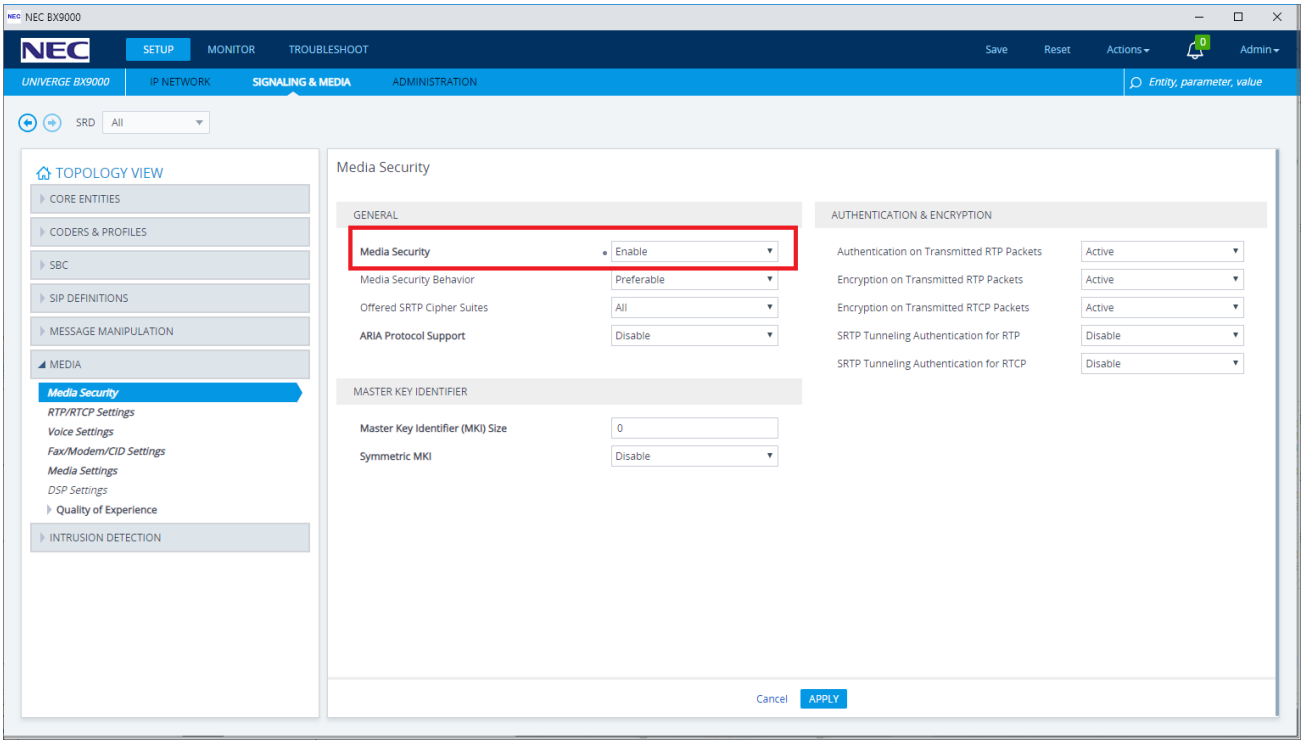
2. Configure an IP Group for MS Teams. No registration is required with the MS Cloud PBX.



Name	Parameter
General	
Name	MS Teams (arbitrary descriptive name)
Topology Location	Up
Type	Server
Proxy Set	MS Teams
IP Profile	MS Teams IP Profile
SBC General	
Classify By Proxy Set	Disabled
Advanced	
Local Host Name	sbc.necdemo.co.uk (change to customer requirements)
Always Use Src Address	Enabled
Message Manipulation	
Proxy Keep-Alive using IP Group settings	Enable
All other parameters can be left unchanged at their default values.	

Enable SRTP Security Transcoding

MS Teams requires the use of SRTP only. The SV9100 IP Profile has RTP enabled, so it is necessary for the SBC to encrypt the RTP Payload. To enable this option ensure that *SETUP > SIGNALING & MEDIA > MEDIA > Media Security > Media Security* is set to Enable.



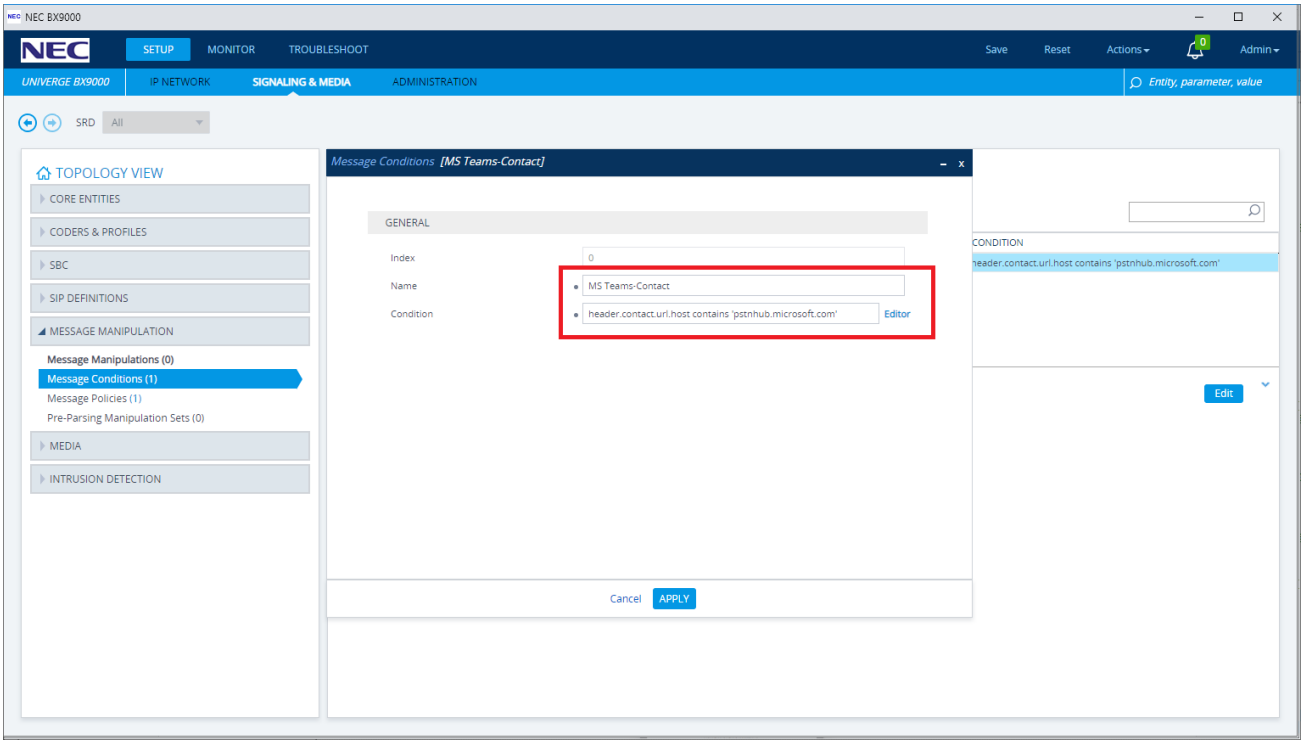
Security transcoding does not change the codec used, but encrypts the RTP payload using the keys exchanged in the Offer/Answer exchange.

Configure Classification conditions

Classification is used to classify incoming SIP dialog-initiating requests with a 'source' IP Group. This source IP Group is then used to route calls between different SIP entities.

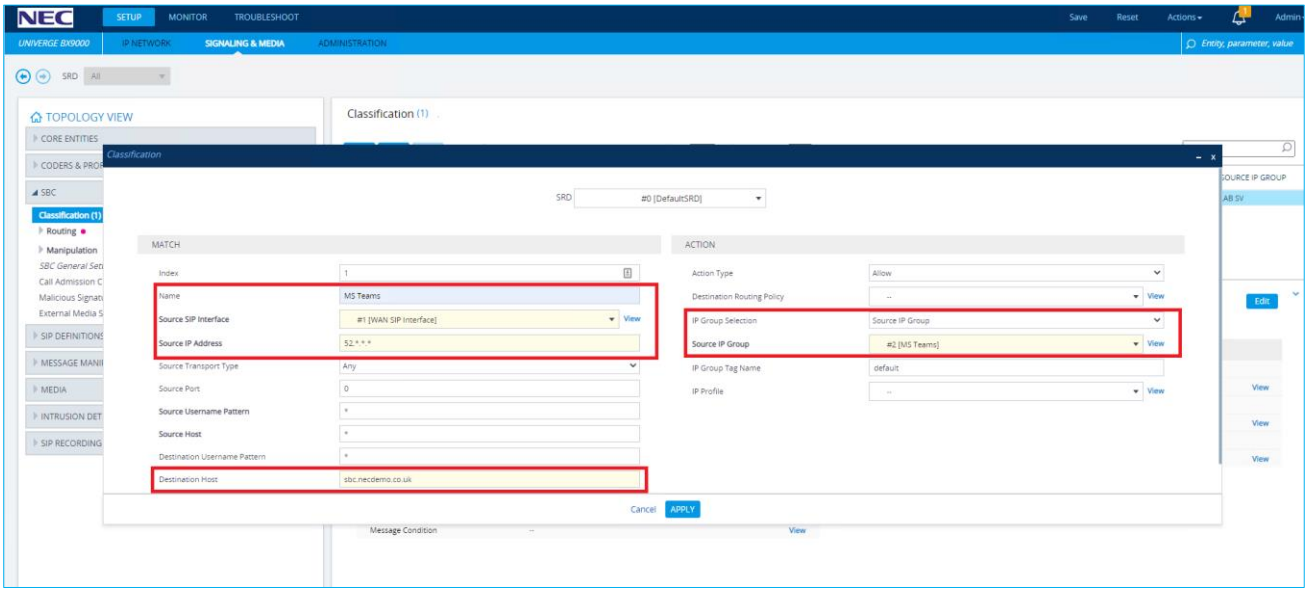
The classification rules are more secure when Message Conditions are included. To create the necessary Classification Rules for MS Teams communication;

1. Navigate to *SETUP > SIGNALING & MEDIA > MESSAGE MANIPULATION > Message Conditions*. Add a new Message Condition with the following condition.



Parameter	Value
Name	MS Teams-Contact (arbitrary descriptive name)
Condition	header.contact.url.host contains 'pstnhub.microsoft.com'

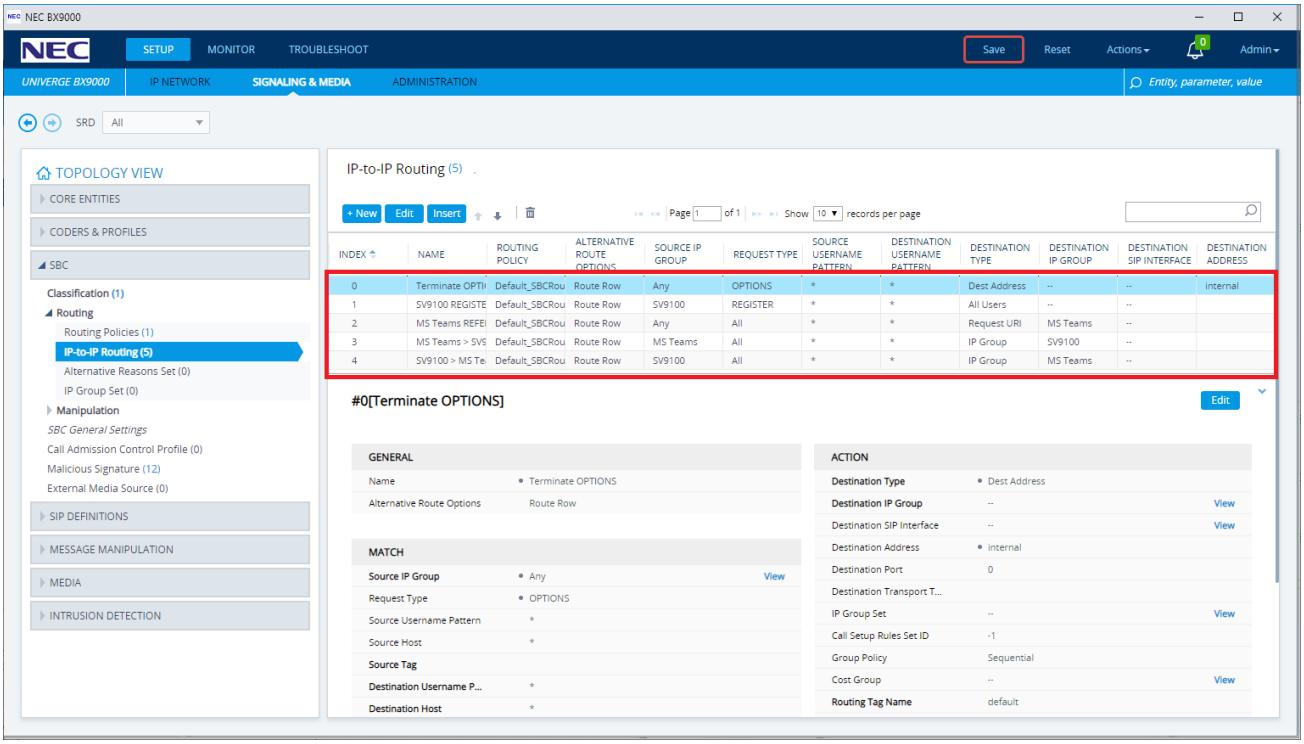
2. Navigate to *SETUP > SIGNALING & MEDIA > SBC > Classification.* Add a new Classification rule for MS Teams with the following conditions to allow known traffic to pass SBC security.



Parameter	Value
Name	MS Teams (arbitrary descriptive name)
Source SIP Interface	WAN SIP Interface
Source IP Address	52.*.*.*
Destination Host	sbc.necdemo.co.uk (setting as per customer SBC FQDN)
Message Condition	MS Team-Contact
Action Type	Allow
Source IP Group	MS Teams

Configure IP-to-IP Routing Rules

This section describes how to configure the necessary IP-to-IP Routing rules for communication between the SV9100 PBX and MS Teams Cloud PBX. These rules may vary depending on other functions of the SBC. As a minimum the rules below should be added or configured.



Index	Name	Source IP Group	Request Type	Call Trigger	ReRoute IP Group	Dest Type	Dest IP Group	Dest Address	Function of this rule?
0	Terminate OPTIONS	Any	OPTIONS	Any	Any	Dest Address	-	internal	This rule terminates received OPTIONS messages for received Keep-Alive messages
1	SV9100 REGISTER	SV9100	REGISTER	Any	Any	All Users	-	-	This rule allows the SBC to respond to REGISTER messages from the SV9100 and authenticate based on the credentials in the IP Group settings
2	MS Teams REFER	Any	All	REFER	MS Teams	Request URI	MS Teams	-	This rule is used to allow MS Teams to transfer calls correctly
3	MS Teams > SV9100	MS Teams	All	Any	Any	IP Group	SV9100	-	This rule routes calls from MS Teams to the SV9100 Tie Trunk
4	SV9100 > MS Teams	SV9100	All	Any	Any	IP Group	MS Teams	-	This rule routes calls from the SV9100 Tie Trunk to the MS Teams Cloud PBX

Please review the necessary dial plan routing between MS Teams and the SV9100. Default routing rules are based on wildcard (*) entries, but these should be restricted to the customer dial plan.

MS Teams Configuration

Connect the SBC to Microsoft Direct Routing

NEC does not provide support for configuration of MS Teams components and the information provided in this section is for guidance only. Care should be taken to review the latest documentation and verify that the detailed commands are correct and appropriate for the MS Teams tenant.

For full documentation of Microsoft Direct Routing review the documentation here;

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-landing-page

Much of the required setup is carried out using Microsoft PowerShell.

Download and install the Skype for Business Online Windows PowerShell Module from here;

https://www.microsoft.com/en-us/download/details.aspx?id=39366

Depending on your MS Teams configuration you will need to follow one of the methods below to connect to the MS Teams Tenant PowerShell session.

1. Connect to MS Teams using an administrator account name and password

```
Import-Module SkypeOnlineConnector
$userCredential = Get-Credential
$sfbSession = New-CsOnlineSession -Credential $userCredential
Import-PSSession $sfbSession
```

This method is used when the administrator account has multi-factor authentication **disabled**.

2. Connect to MS Teams using an administrator account with multi-factor authentication enabled.

```
Import-Module SkypeOnlineConnector
$sfbSession = New-CsOnlineSession
Import-PSSession $sfbSession
```

This method is used when MFA is enabled, you will need to verify your credentials by email or SMS service.

Create the SBC gateway

Validate the commands used to create the SBC gateway using this command;

```
Get-Command *onlinePSTNGateway*
```

These commands are used to manage the link to the customer on premise SBC.

```
CommandType     Name                           Version    Source
-----------     ----                           -------    ------
Function        Get-CsOnlinePSTNGateway        1.0        tmp_v5fiu1no.wxt
Function        New-CsOnlinePSTNGateway        1.0        tmp_v5fiu1no.wxt
Function        Remove-CsOnlinePSTNGateway     1.0        tmp_v5fiu1no.wxt
Function        Set-CsOnlinePSTNGateway        1.0        tmp_v5fiu1no.wxt
```

Use the following command to connect the SBC to the tenant;

```
New-CsOnlinePSTNGateway -Identity sbc.necdemo.co.uk -Enabled $true -SipSignalingPort
5061 -MaxConcurrentSessions 10
```

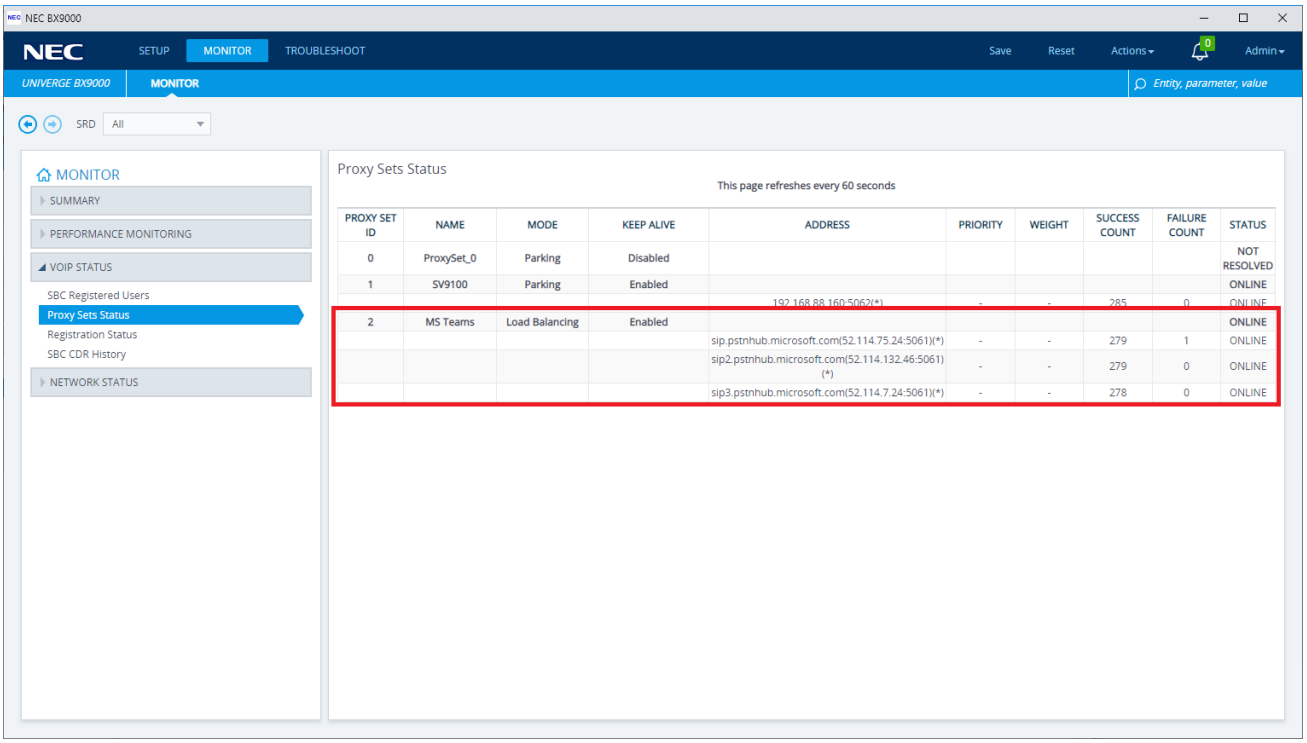
This command will create a SIP link to sbc.necdemo.co.uk:5061 and support a maximum of 10 concurrent calls.

You can verify the gateway is enabled using the following command;

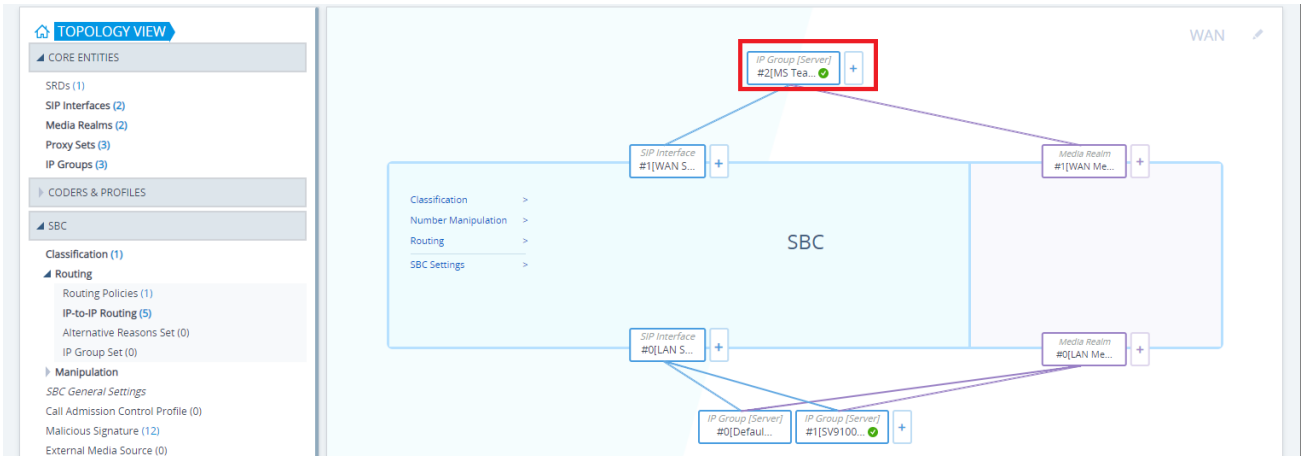
```
Get-CsOnlinePSTNGateway -Identity sbc.necdemo.co.uk
```

Verify the link in the SBC Status pages

To verify the online status of the MS Teams connector, navigate to *MONITOR > VOIP STATUS > Proxy Sets Status*.



You can also see the status of the IP Group in *SETUP > SIGNALING & MEDIA > TOPOLOGY VIEW*.



Enable the users for Enterprise Voice and assign on premise PSTN number

To enable the MS Teams user for voice, ensure that they have a license assigned which includes Teams (i.e. E1, E3, E5) plus the Microsoft Phone System license.

** Please be aware this license can take several hours to allocate – during testing it took more than 6 hours between allocating in the administration centre and activation.

Using PowerShell issue the following command;

```
 Set-CsUser -Identity "<User name>" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true
-OnPremLineURI tel:<E.164 phone number>
```

For example;

```
Set-CsUser -Identity "dave.smith@necdemo.co.uk" -OnPremLineURI tel:+441159695700 -
EnterpriseVoiceEnabled $true -HostedVoiceMail $true
```

This must be the full E.164 formatted number. For more information see https://www.itu.int/rec/T-REC-E.164-201011-I/en

Configure Voice Routing

Create the PSTN Usage

In this example only a single usage is created. For more complex plans see Microsoft documentation. Using PowerShell create a PSTN Usage called 'NEC' using this command;

```
Set-CsOnlinePstnUsage -Identity Global -Usage @{Add="NEC"}
```

Verify this is created using this command;

```
(Get-CsOnlinePstnUsage).usage
```

Create an Online Voice Route

The Online Voice Route is a regex pattern which matches a dialled number to the PSTNGateway and PSTN Usage. In this example there is a single Online Voice Route called 'NEC SBC' which matches all dialled digits (.*), is linked to the PSTN Gateway 'sbc.necdemo.co.uk' and PSTN Usage called 'NEC'.

```
New-CsOnlineVoiceRoute -Identity "NEC SBC" -NumberPattern ".*" -
OnlinePstnGatewayList sbc.necdemo.co.uk -Priority 1 -OnlinePstnUsages "NEC"
```

You can verify this using the command;

```
Get-CsOnlineVoiceRoute
```

```
Identity             : NEC SBC
Priority             : 1
Description          :
NumberPattern        : .*
OnlinePstnUsages     : {NEC}
OnlinePstnGatewayList : {sbc.necdemo.co.uk}
Name                 : NEC SBC
```

Create a new Voice Routing Policy

The Voice Routing Policy is used to link a user to the Online Voice Route. Again in this example there is a single Policy called 'NEC SBC' and links to PSTN Usage 'NEC' using this command;

```
New-CsOnlineVoiceRoutingPolicy "NEC SBC" -OnlinePstnUsages "NEC"
```

You will see confirmation of the new routing policy as below;

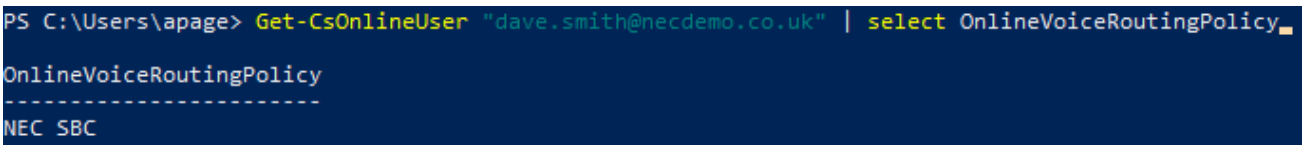
```
Identity            : Tag:NEC SBC
OnlinePstnUsages    : {NEC}
Description         :
RouteType           : BYOT (Bring Your Own Trunk)
```

The final step is to assign this policy to our users. This can be done with this command;

```
Grant-CsOnlineVoiceRoutingPolicy -Identity "dave.smith@necdemo.co.uk" -PolicyName
"NEC SBC"
```

And this can be verified with the following command;

```
Get-CsOnlineUser "dave.smith@necdemo.co.uk" | select OnlineVoiceRoutingPolicy
```

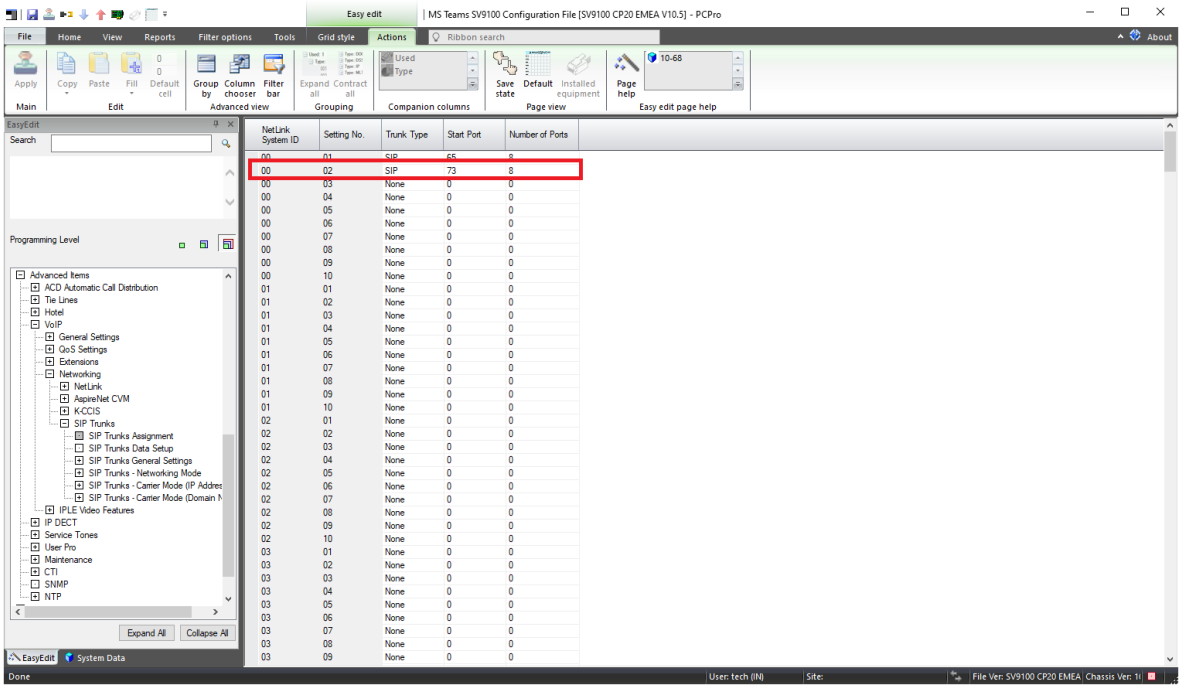


SV9100 Configuration

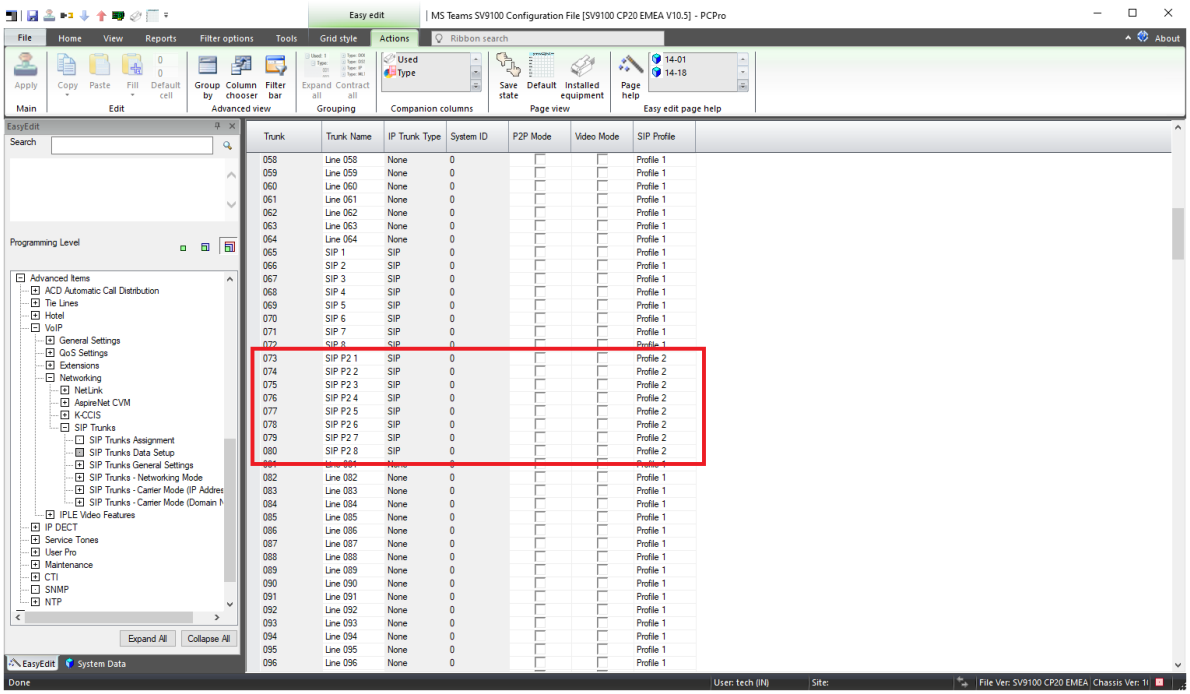
IP Trunk Setup

Using the PCPro application complete the following steps to setup a Tie-line trunk to the BX Series SBC. This example is based on using SIP Trunking Profile 2, and assuming the customer may already have IP Trunks directly connected using IP Profile 1. If you want to use IP Profile 1 you will need to adjust the settings in this section.

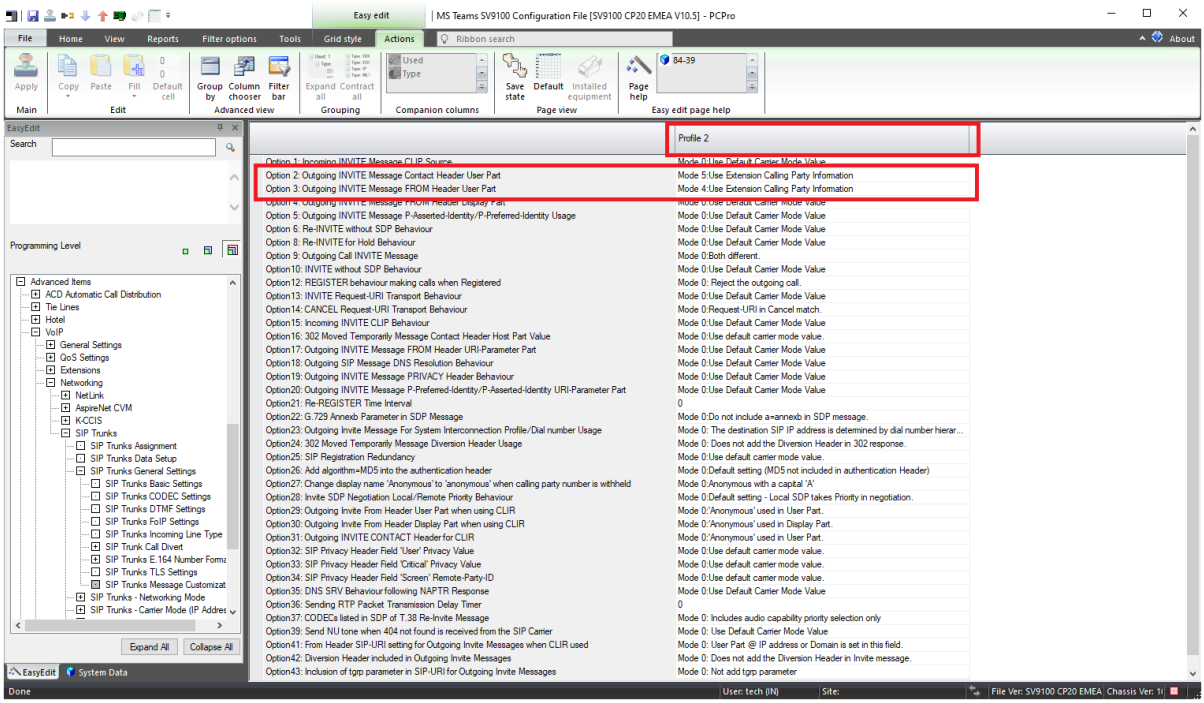
1. Create SIP Trunks for the interconnection. In *Advanced Items + VoIP + Networking + SIP Trunks + SIP Trunks Assignment* assign the trunks. Ensure that you have the correct number of IP Trunk licenses installed before completing this step.



2. Assign the SIP trunks to IP Profile 2.

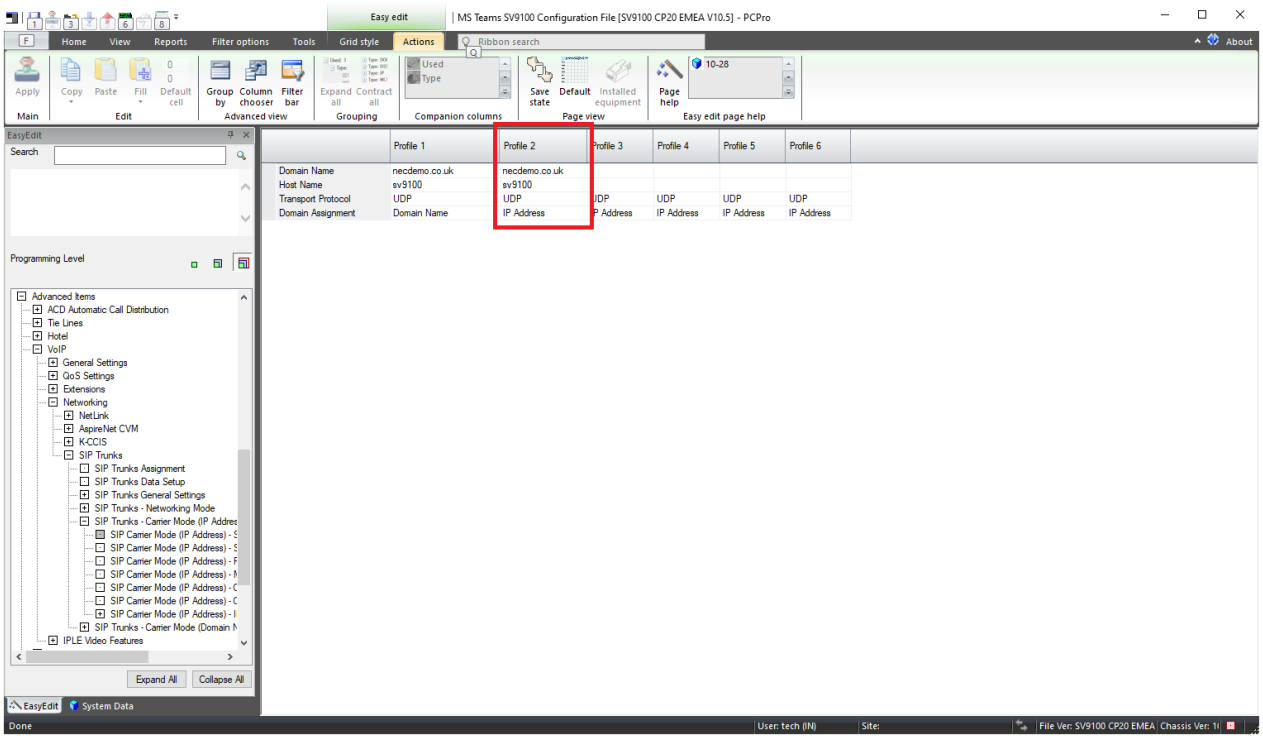


3. Modify the SIP Customisation Options for Profile 2 in *Advanced Items + VoIP + Networking + SIP Trunks + SIP Trunks General Settings + SIP Trunks Message Customization*.

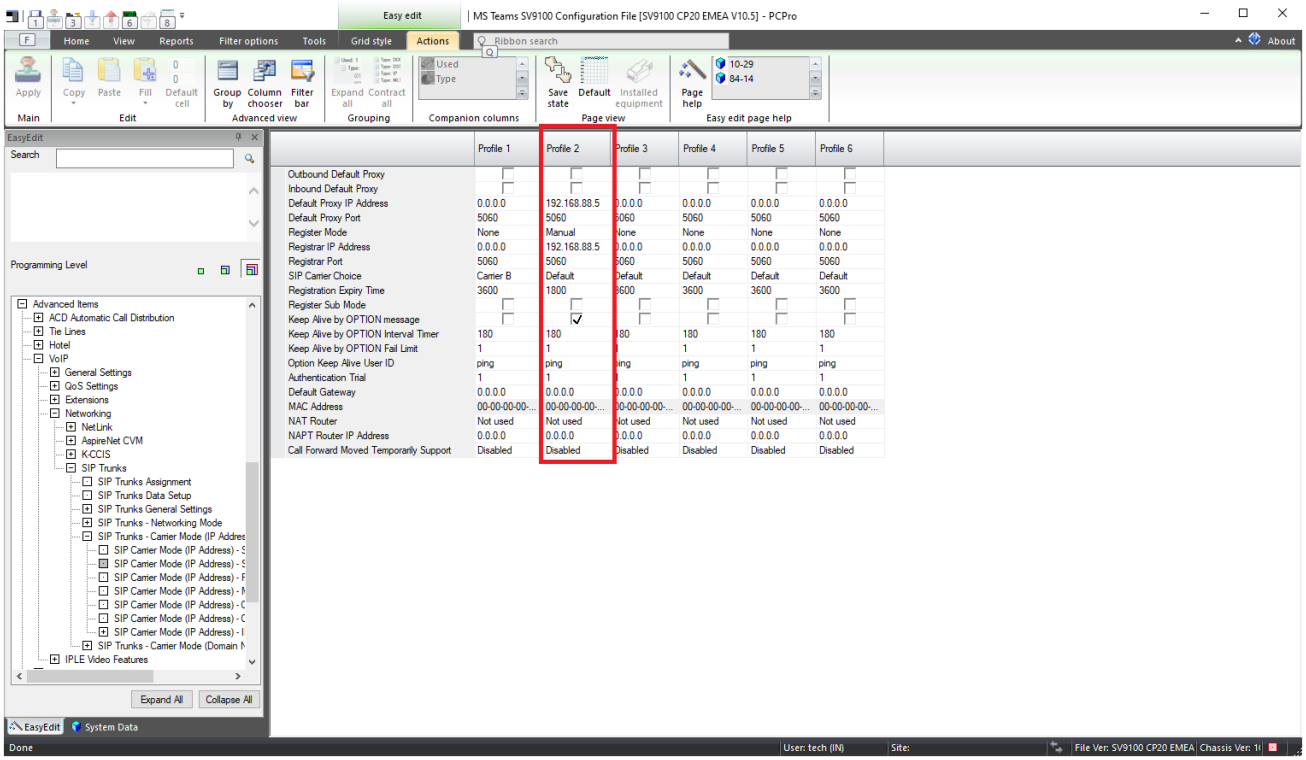


	Profile 2
Option 2: Outgoing INVITE Message Contact Header User Part	Mode 2:Use Calling Party Information
Option 3: Outgoing INVITE Message FROM Header User Part	Mode 1:Use Calling Party Information
Option 4: Outgoing INVITE Message FROM Header Display Part	Mode 2:Use Calling Party Information

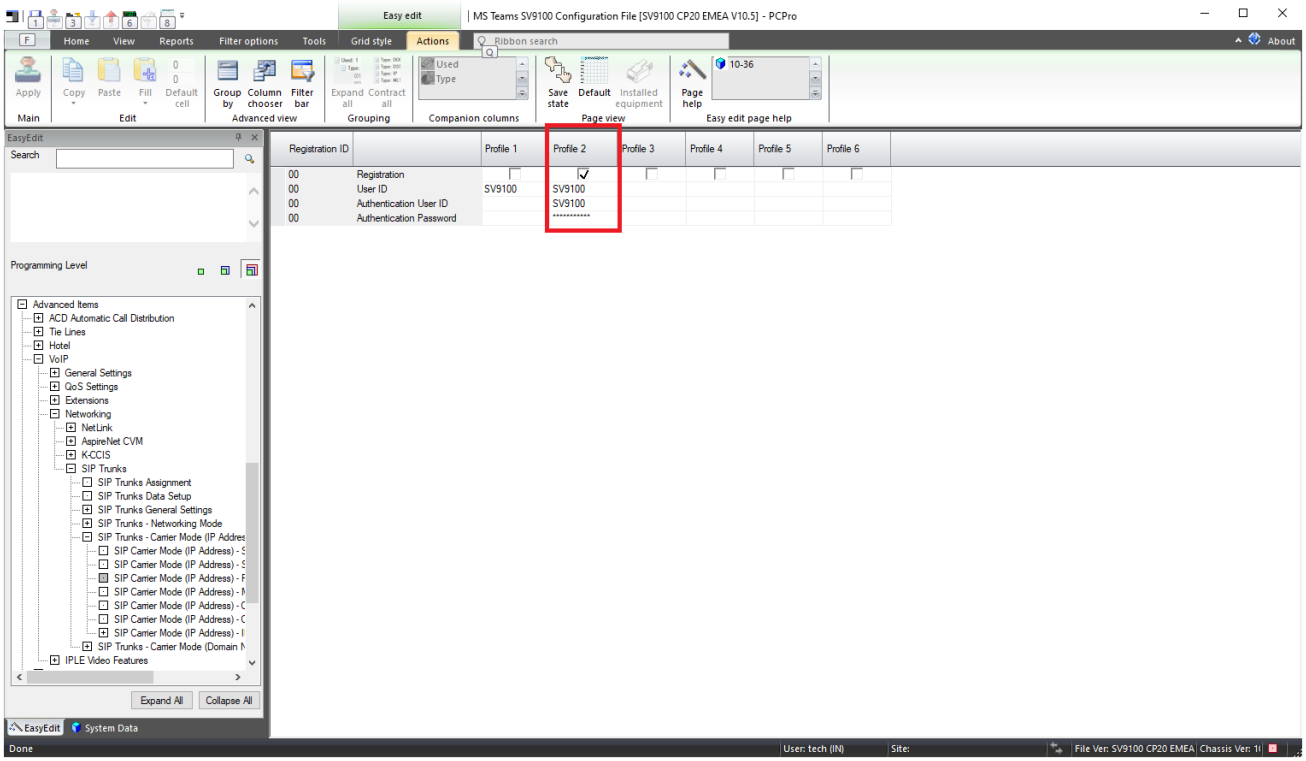
4. Configure the SIP Host, Domain and Transport Protocol for Profile 2 with your customer information in *Advanced Items + VoIP + Networking + SIP Trunks + SIP Trunks - Carrier Mode (IP Address) + SIP Carrier Mode (IP Address) - System Information Setup*.



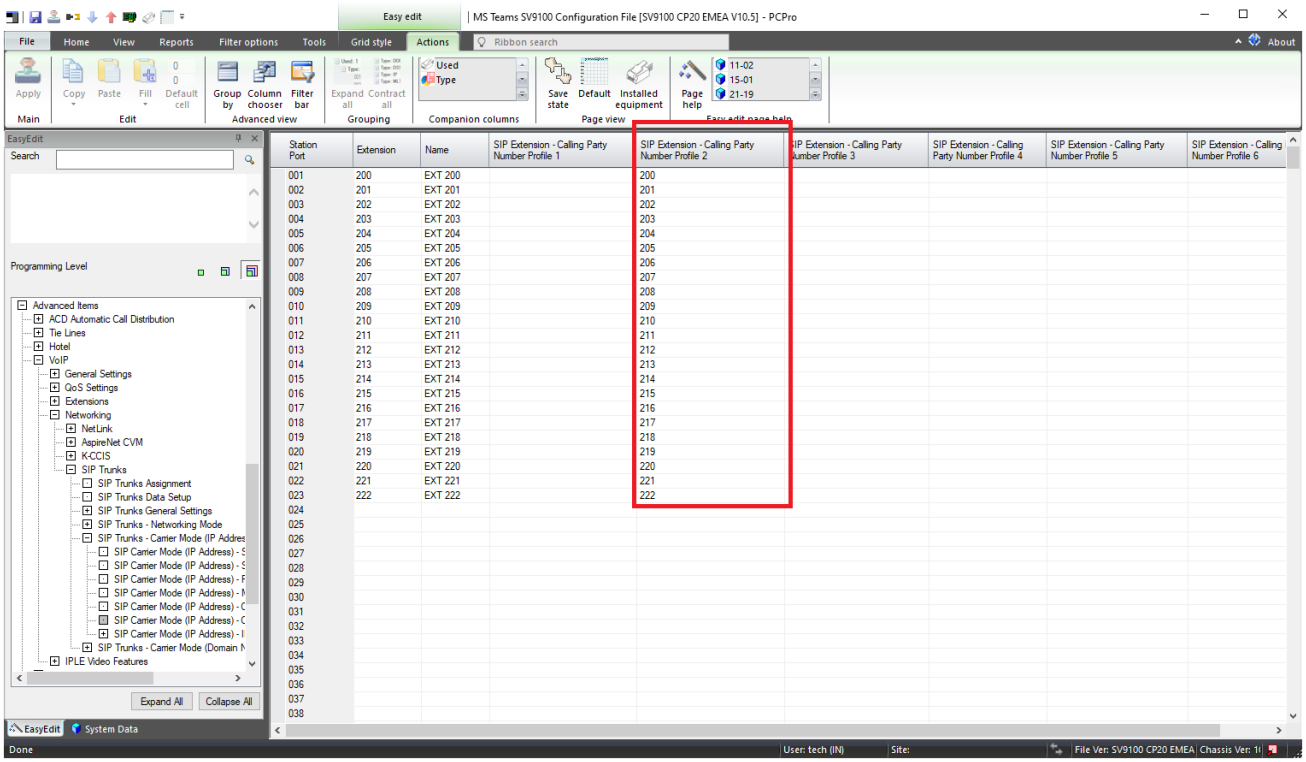
5. Configure the SIP Server connection to the SBC. Replace the IP address with the LAN IP address of the BX SBC in *Advanced Items + VoIP + Networking + SIP Trunks + SIP Trunks - Carrier Mode (IP Address) + SIP Carrier Mode (IP Address) - Server Setup*. Ensure that Register Mode is set to Manual.



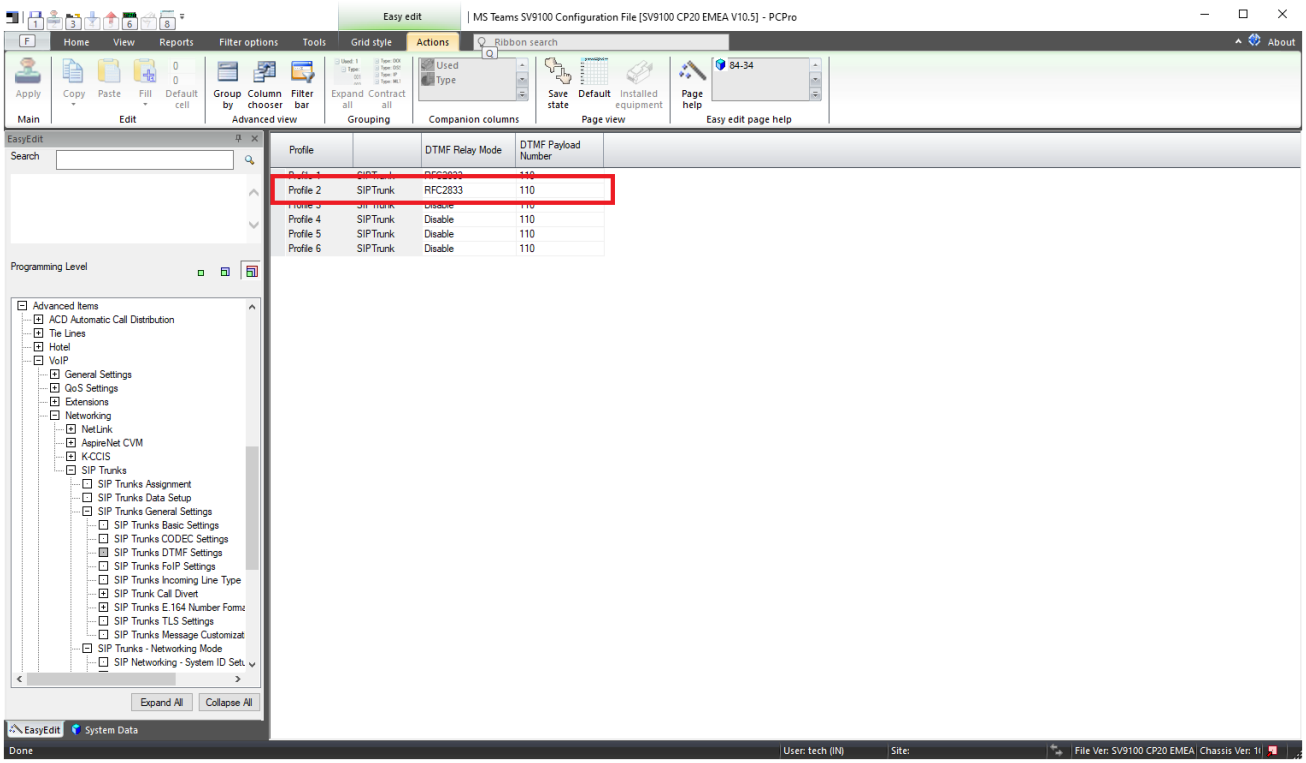
6. Configure the SIP Registration account defined in the SV9100 IP Group on the SBC. Add your credentials in *Advanced Items + VoIP + Networking + SIP Trunks + SIP Trunks - Carrier Mode (IP Address) + SIP Carrier Mode (IP Address) - Primary Authentication Information*



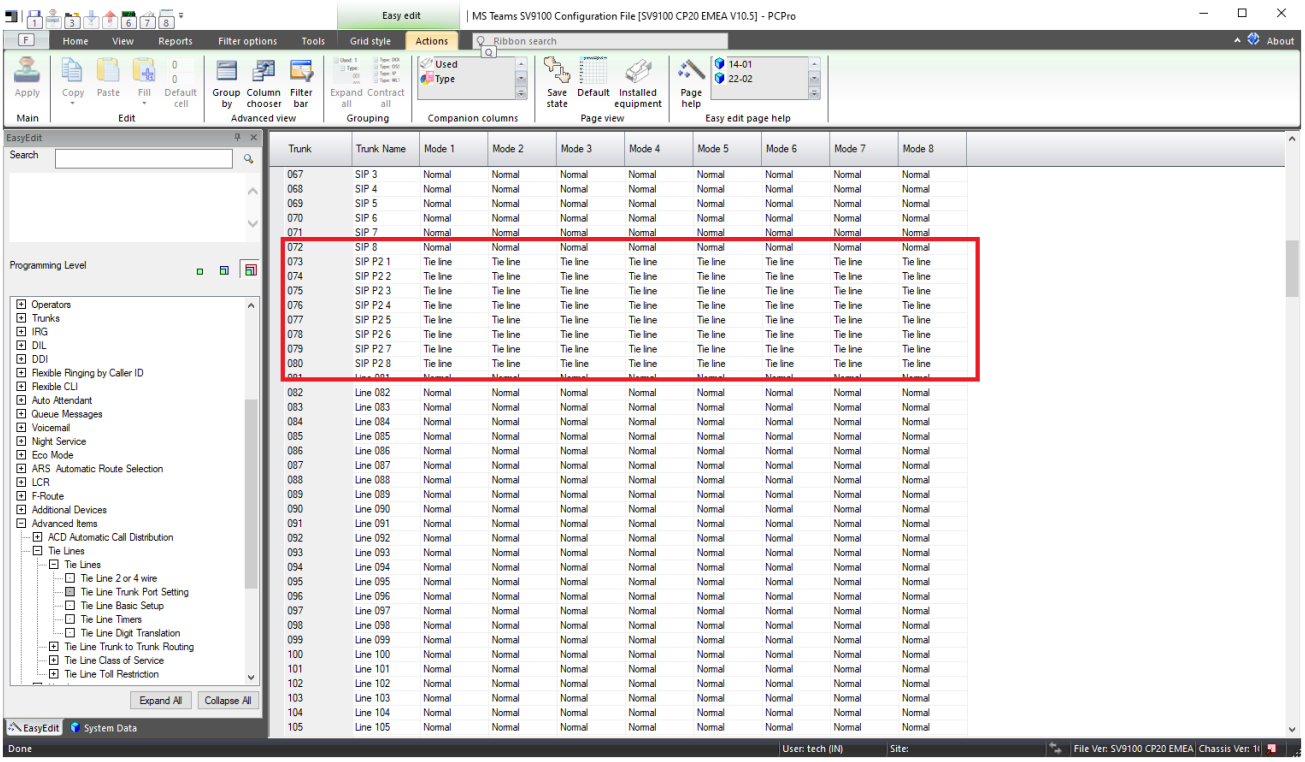
7. Set your CPN to display the number sent towards MS Teams. For example this could be the extension number, or it may include branch office access codes (for redial). **This item must be set!**



8. Configure DTMF support for the SIP tie-line in *Advanced Items + VoIP + Networking + SIP Trunks + SIP Trunks General Settings + SIP Trunks DTMF Settings.*



9. Set your Incoming Trunks to Tie Line mode in *Advanced Items + Tie Lines + Tie Lines + Tie Line Trunk Port Setting*. When this item is set then incoming calls are referenced against the System Numbering Plan.

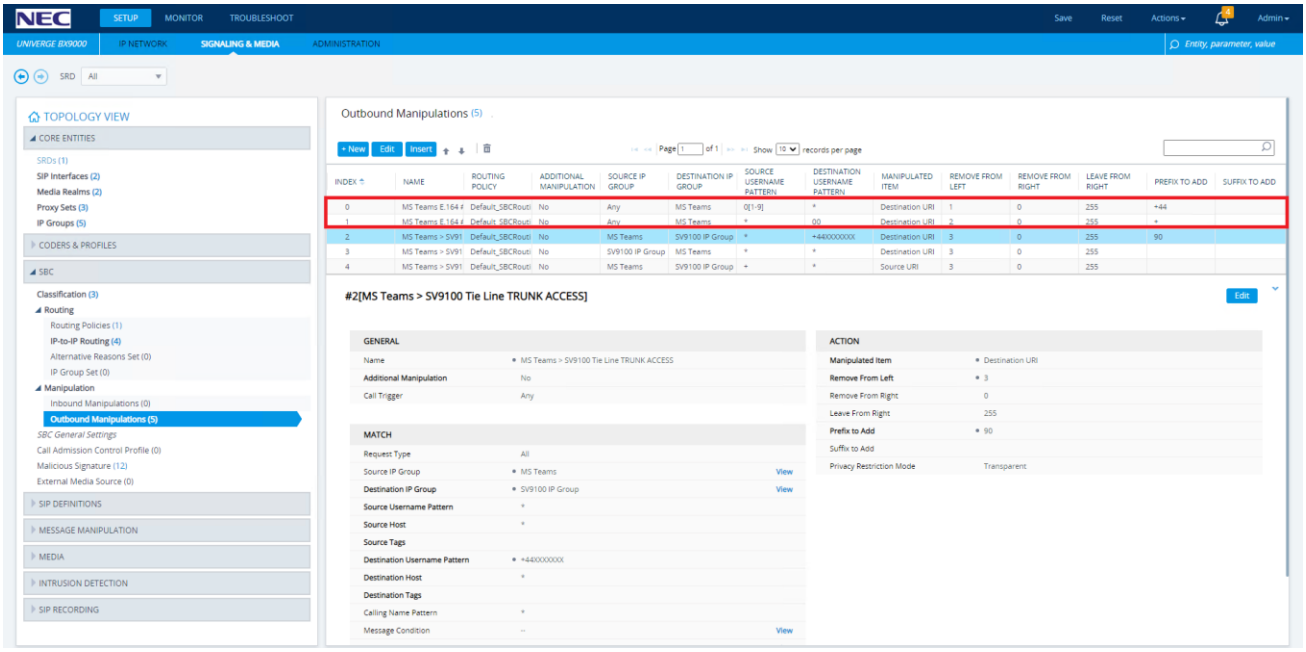


Configure Number Manipulation Rules

For calls from SV9100 to MS Teams

When placing a call to MS Teams it is necessary to use E.164 numbering scheme. The default behaviour of the SV9100 is to send the number as dialled. The easiest place to modify this is in the SBC.

The example below removes the leading 0 digit and replaces it with +44 (replace with local country code), and if 00 is dialled then this is replaced with +.



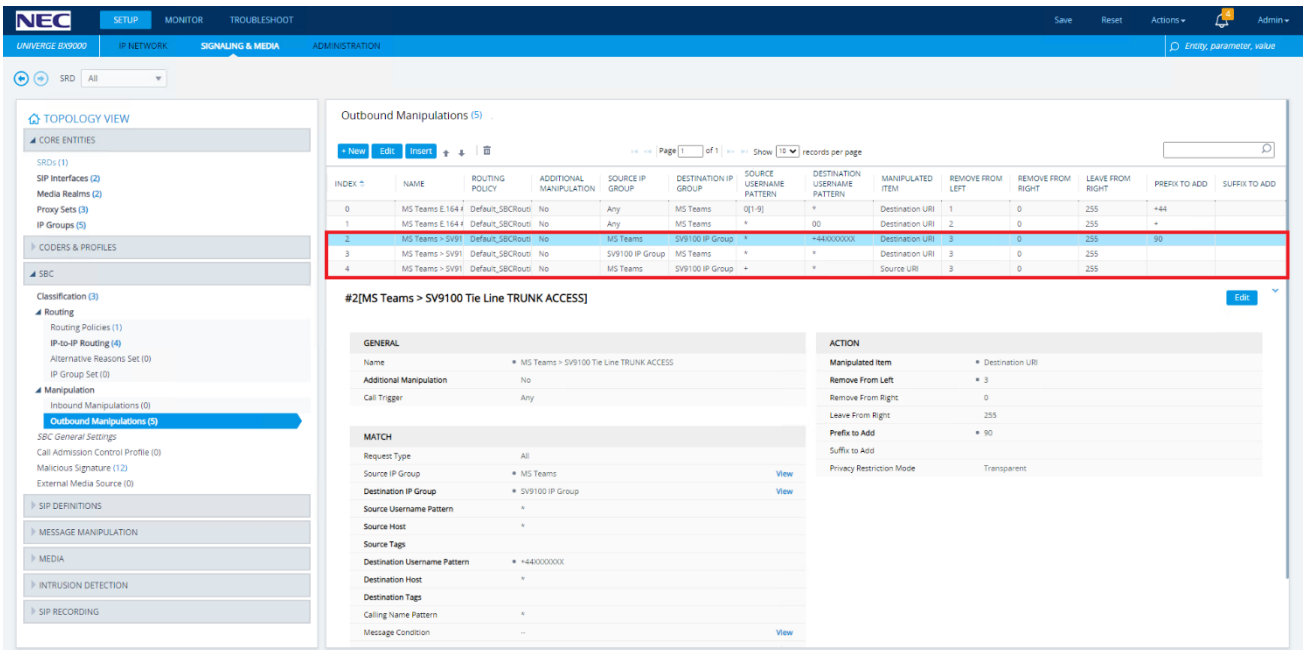
Index	Name	Source IP Group	Dest. IP Group	Dest. Username Pattern	Manipulated Item	Remove from the Left	Prefix to Add	Function of this rule?
0	MS Teams E.164 #1	Any	MS Teams	0[1-9]	Destination URI	1	+44	This rule will remove one digit from the front of the number when a national number is dialled.
1	MS Teams E.164 #2	Any	MS Teams	00	Destination URI	2	+	This rule removes the international prefix and replaces with +

For Calls from MS Teams to SV9100

For calls towards the SV9100 we need to also modify the number format. In this case we need to modify both the Source and Destination URI.

Again, this example is based on country code 44 and a station numbering plan of 2XX on the SV9100.

You may need to modify these rules to suit your numbering plan.



Index	Name	Source IP Group	Dest. IP Group	Source Username Pattern	Dest. Username Pattern	Manipulated Item	Remove from the Left	Prefix to Add	Function of this rule?
2	MS Teams > SV9100 Tie Line TRUNK ACCESS	MS Teams	SV9100	*	+44XXXXXXX	Destination URI	3	90	*Optional* This rule is used when PSTN breakout through the SV9100 is required. It will add the trunk access code 9 and also normalise the PSTN dialled number.**
3	MS Teams > SV9100 Tie Line DEST	MS Teams	SV9100	*	+442XX	Destination URI	3		This rule will remove the +44 in front of the dialled PBX number
4	MS Teams > SV9100 Tie Line SOURCE	MS Teams	SV9100	+	*	Source URI	3	0	This rule normalises the received number from E.164 to national format

** Additional settings are required for PSTN breakout. See section later in this document.

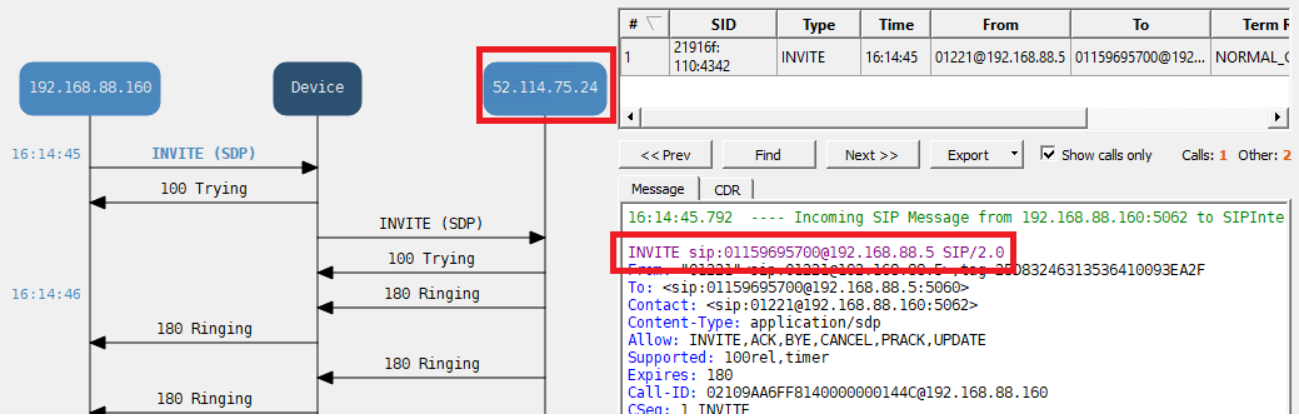
Test the SIP trunk between MS Teams and SV9100

Dialling from the SV9100 to MS Teams

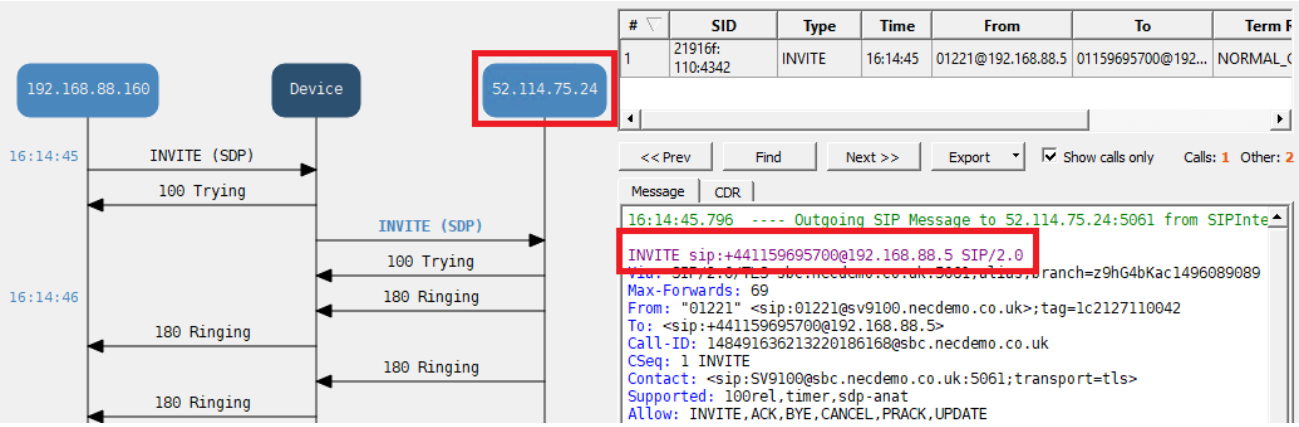
To test the SIP trunk connection between MS Teams and SV9100 select the IP trunk. You can use the default service code 805 (check codes for your region) followed by the trunk number.

For example, 805 073 will select IP Trunk #73. Dial the PSTN number of the MS Teams user.

Here we can see a request from the SV9100 @ 192.168.88.160 towards the SBC;

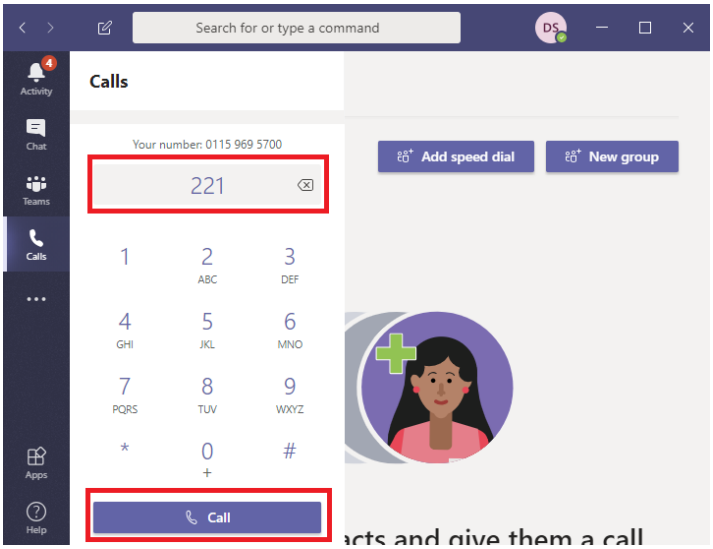


Outbound Number Manipulation is then carried out on the outbound leg towards MS Cloud PBX.

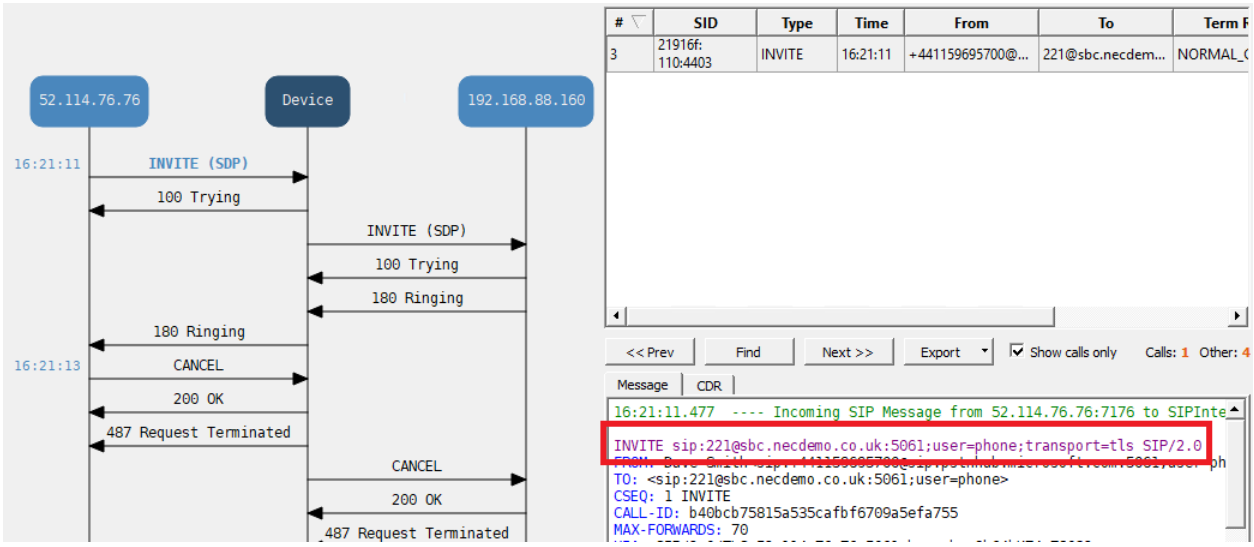


Dialling from MS Teams to SV9100

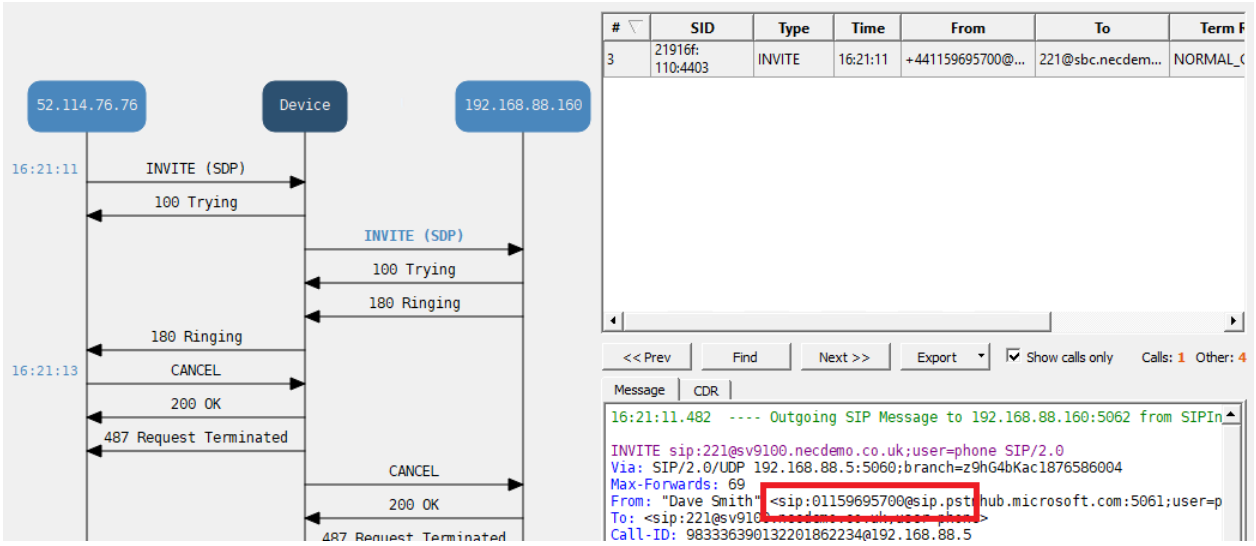
Use the MS Teams client to make a call to one of your SV9100 PBX Extensions.



Here we can see the inbound request from MS Teams Cloud PBX;



And the number is normalised by the Outbound Number Manipulation Rules towards the SV9100



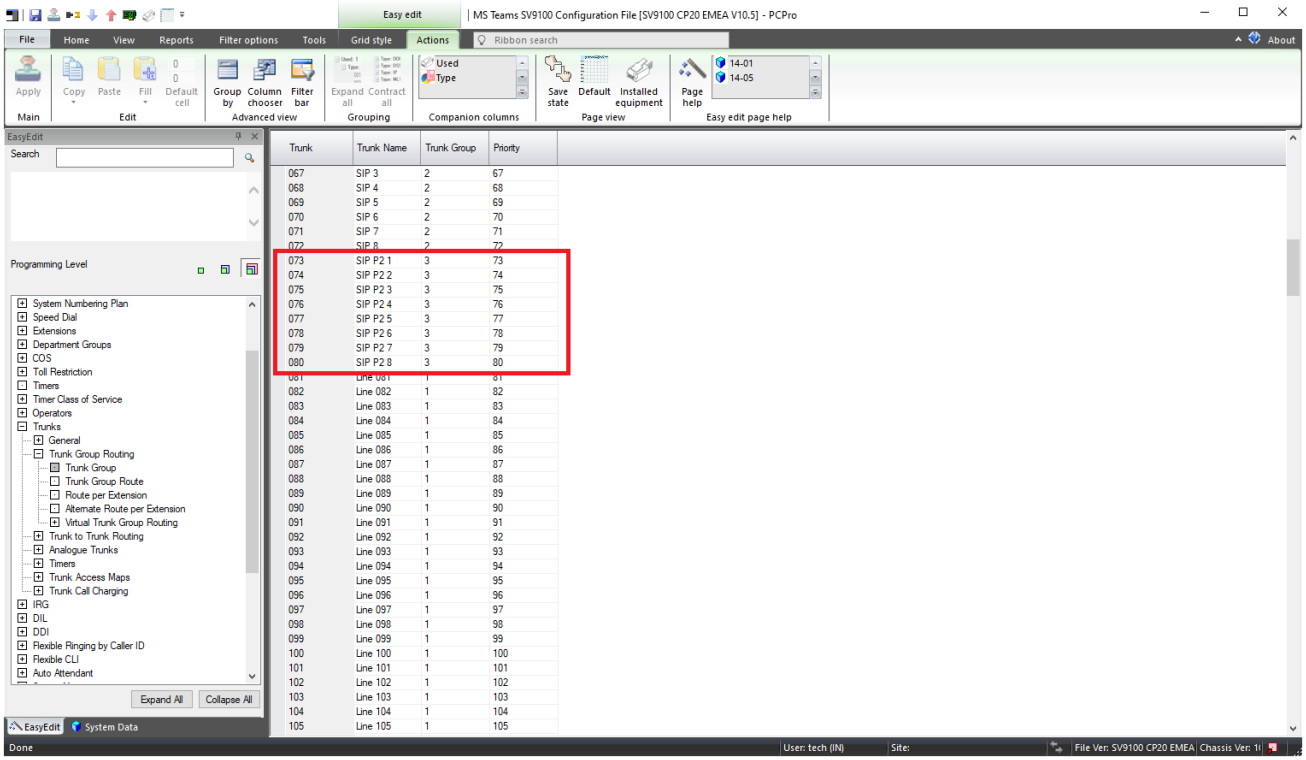
Configure F-Route

F-Route allows quick dialling of MS Teams users from the SV9100 system. In this example the numbers below are used;

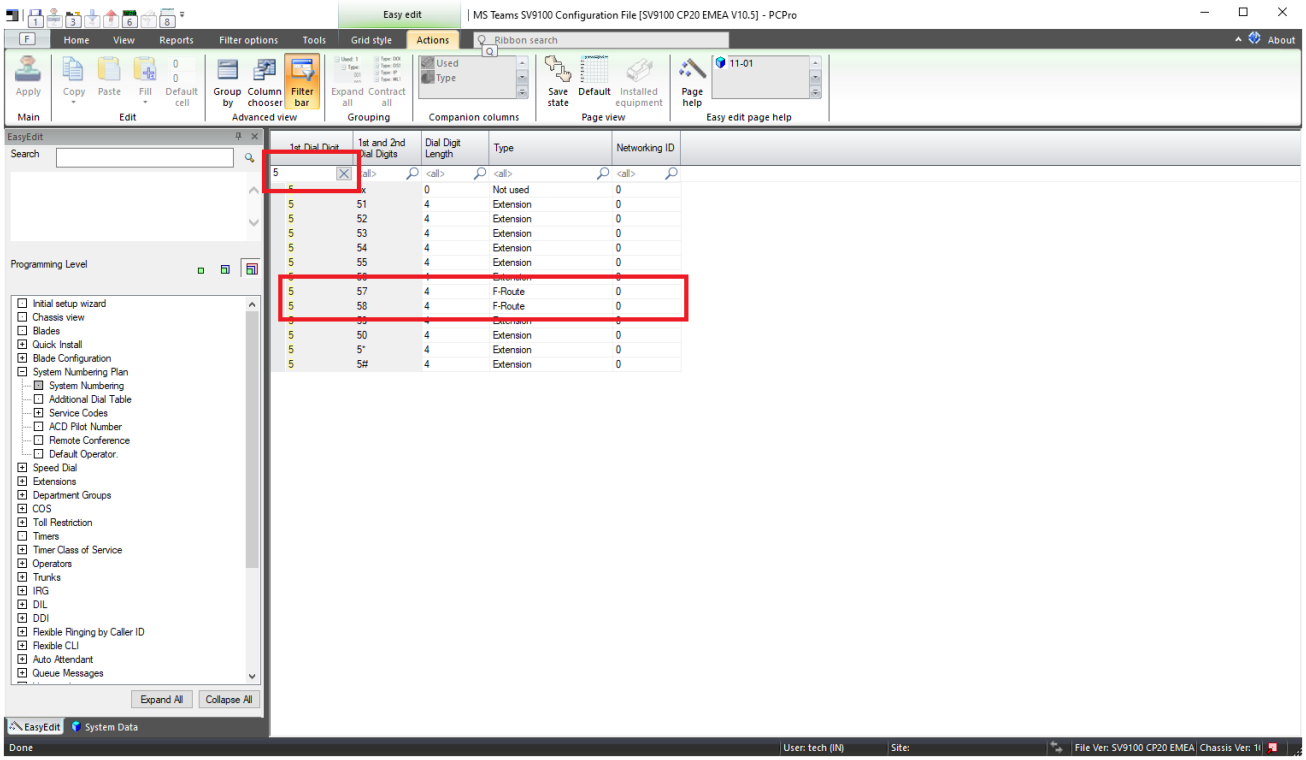
MS Teams User PSTN Number **+44 115 9695700**
Number required to dial from SV9100 **01159695700** on SIP Trunks Profile 2
F-Route number **5700**

So this means that we can implement a rule in the SV9100 to modify dialled number 57xx into 011596957xx and dial on SIP trunks towards the MS Teams Direct Routing connection.

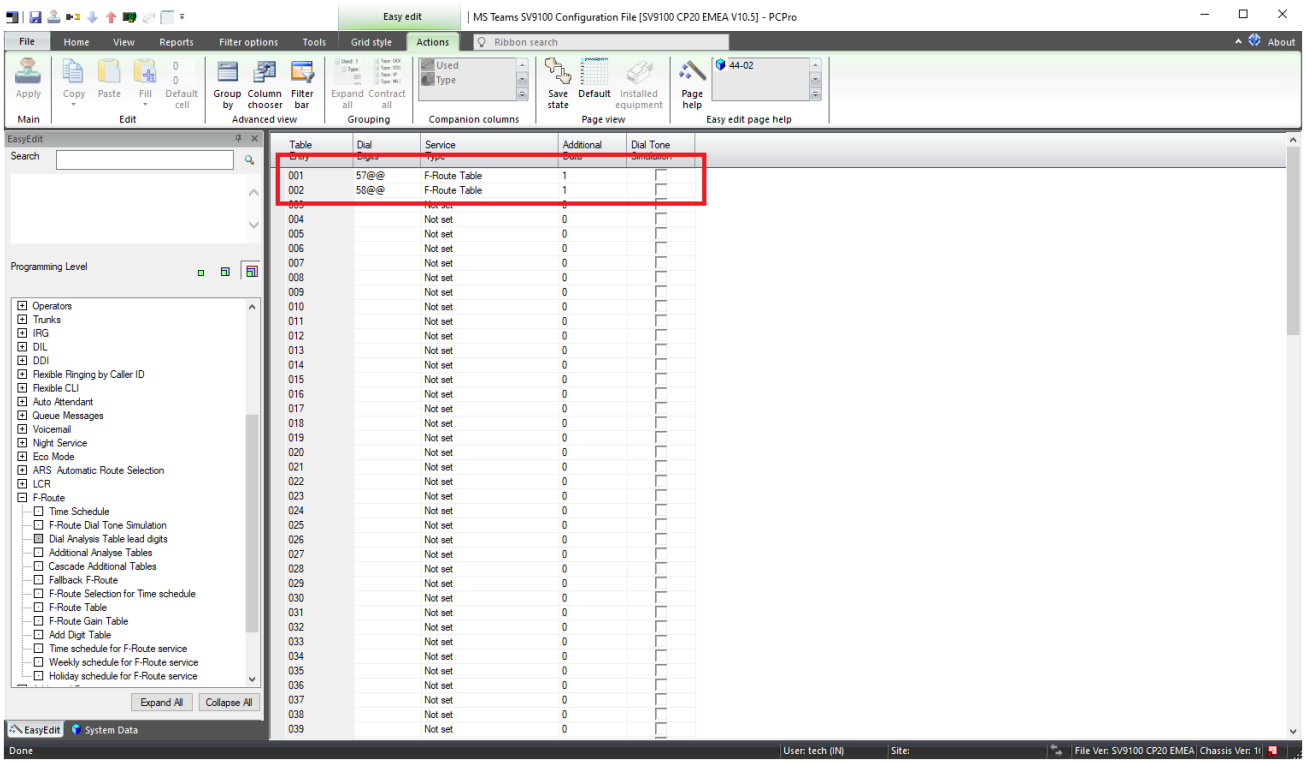
1. Group the SIP Tie Line Trunks in *Trunks + Trunk Group Routing + Trunk Group*. Add the created trunks into an unused trunk group (3 is used here).



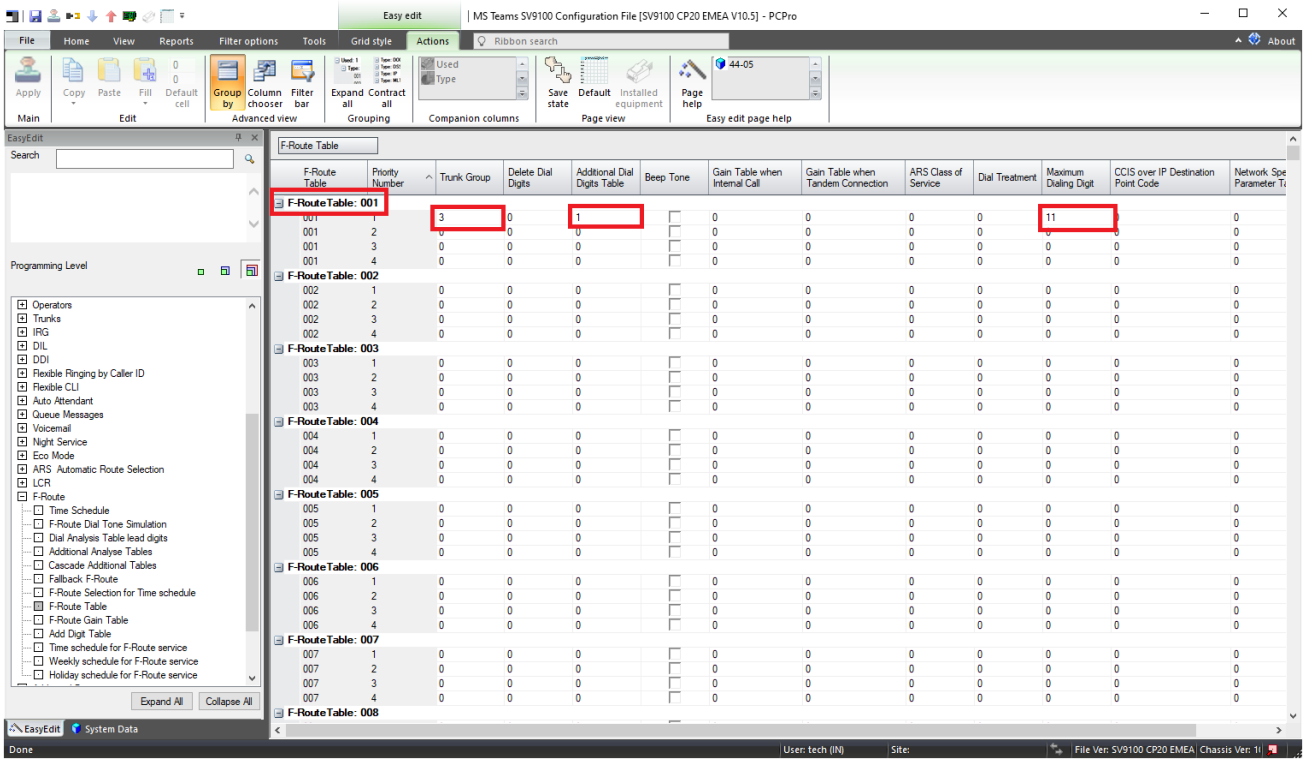
2. Modify your system numbering plan in *System Numbering Plan + System Numbering*. In my example 57 and 58 are four digit F-Route numbers.



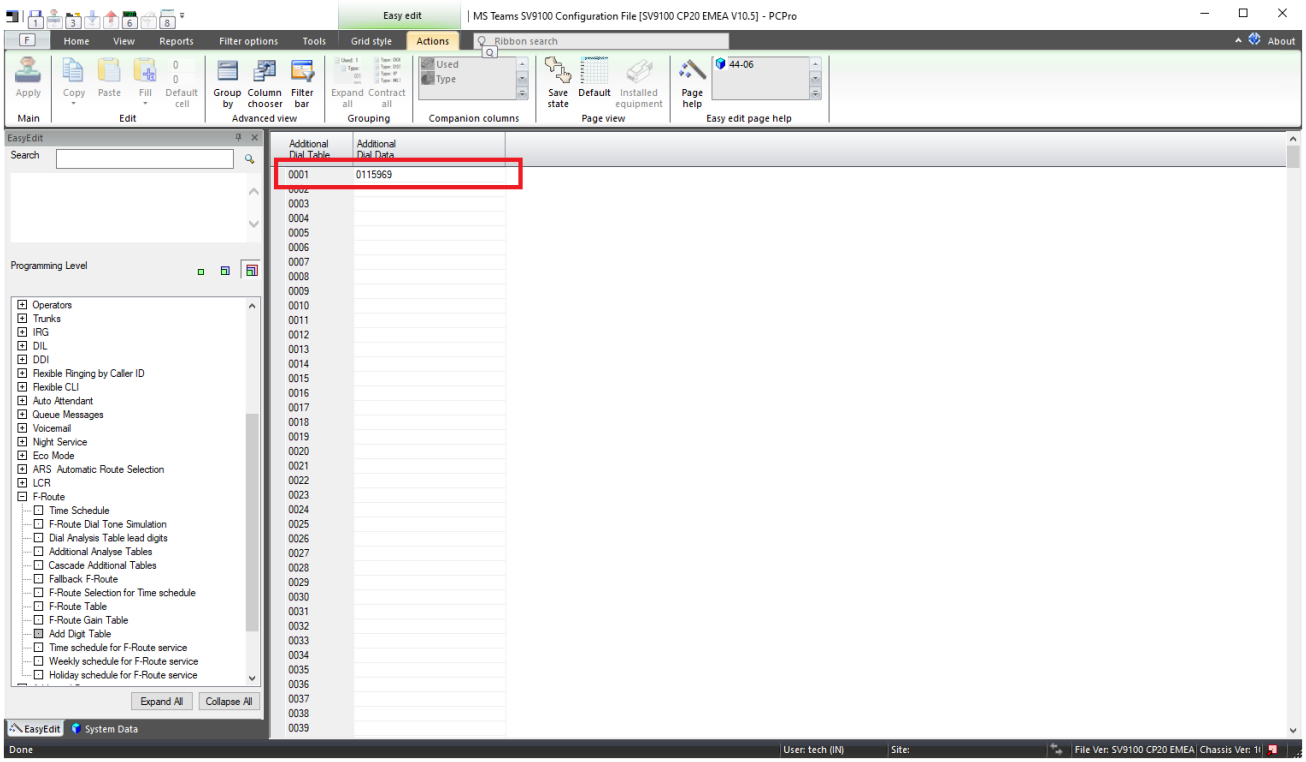
3. Configure the F-Route dialled lead digits in *F-Route + Dial Analysis Table lead digits*. In this example any digits dialled in the range 5700-5799 and 5800-5899 will go to F-Route Table number 1.



4. Configure F-Route Table number 1 to route the dialled number to Trunk Group 3 for the SIP tie-lines and include an Additional Dial Table to complete the full PSTN number. This is programmed in *F-Route + F-Route Table*. Also set the maximum number of Dialling Digits to the same as the PSTN number (11) to eliminate dialling delay.



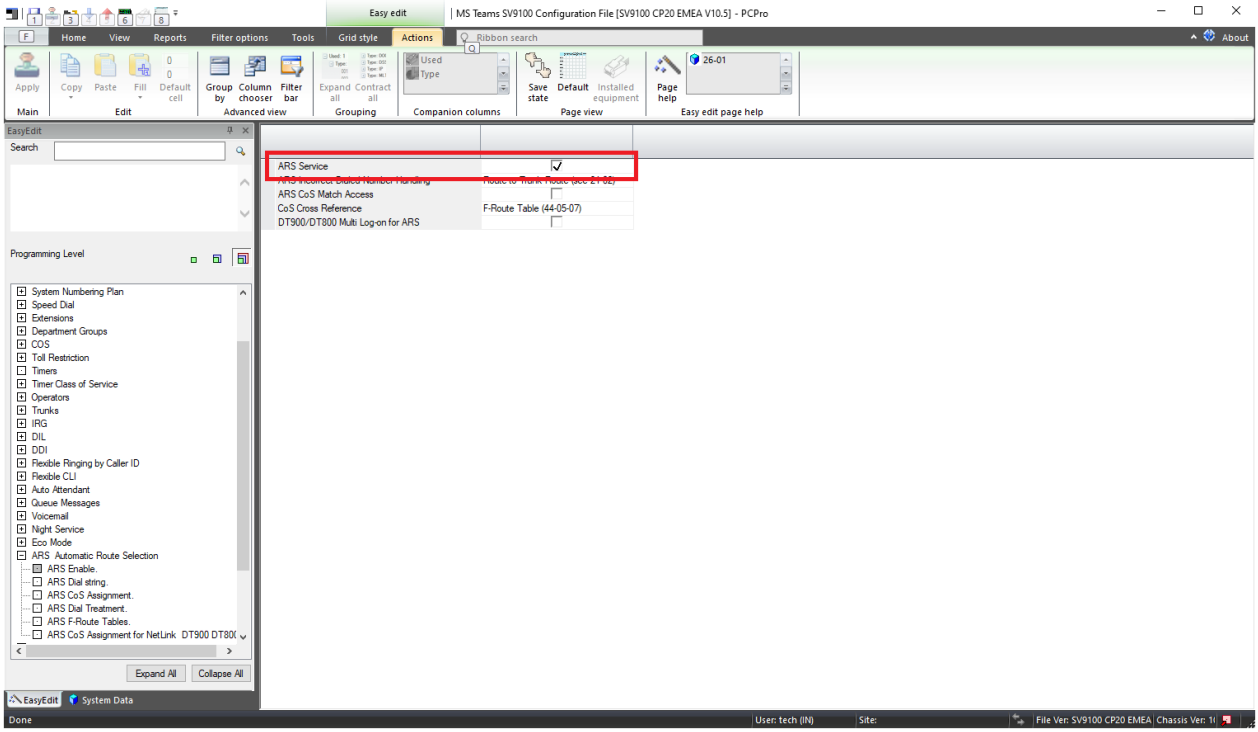
5. Use the Additional Digit Tables to complete the PSTN number which should be dialled. Example - If the user dials 5701 then this will send 01159695701 towards the SIP tie-line. This is programmed in *F-Route + Add Digit Table*.



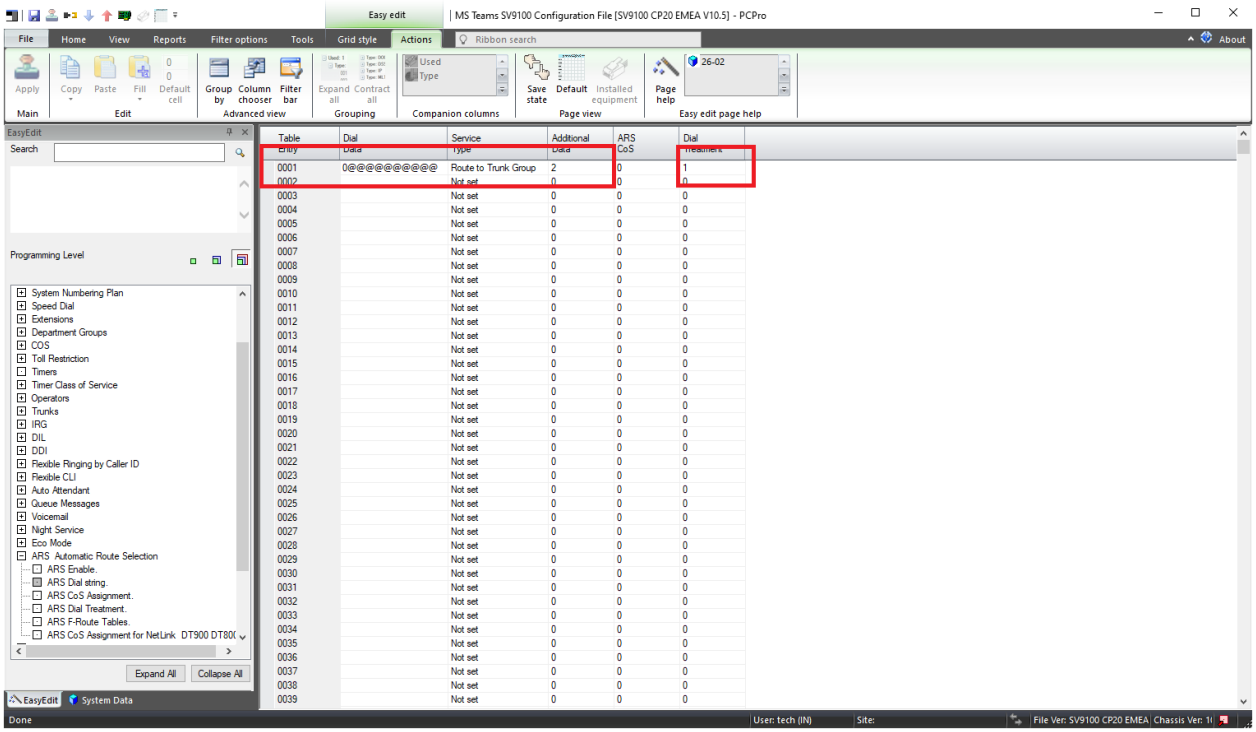
Configure ARS to remove dial delays – Optional

If you are using the SV9100 as a transit system, so calls are made from MS Teams > Direct Routing > SV9100 > PSTN and the PSTN trunks connected to the SV9100 are also SIP, then you will have a delay on the outgoing call leg. You can use ARS to analyse the digits dialled and eliminate the call delay.

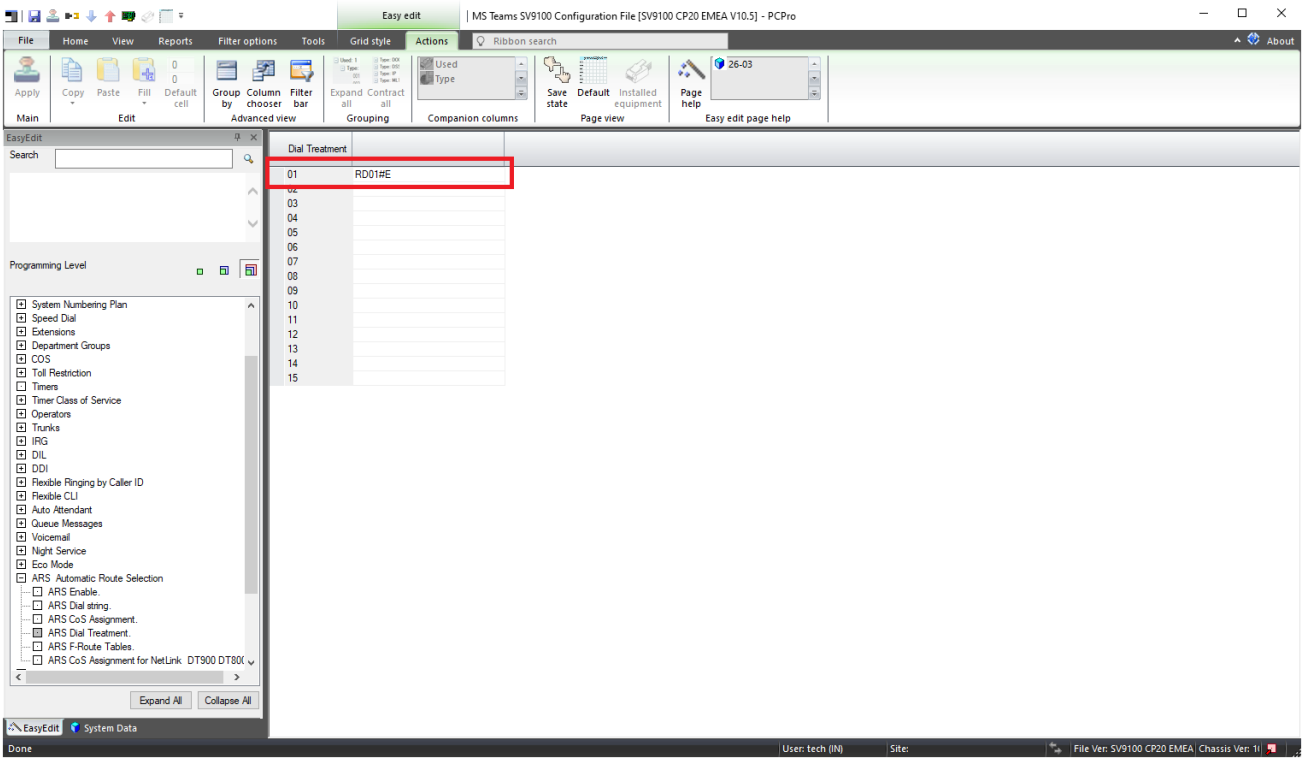
1. Enable the ARS service in *ARS Automatic Route Selection + ARS Enable*.



2. Configure a dial string analysis table in *ARS Automatic Route Selection + ARS Dial string.* This table must be modified to suit your local region. For example UK national numbers start with 0 and are 11 digits in length. The trunk group is the PSTN trunk group connected to the SV9100.



3. Configure the Dial Treatment in *ARS Automatic Route Selection + ARS Dial Treatment*. This treatment will **R**edial **D**ial **01** additional digits, which is **#** and then **E**nd the dial treatment. This means that SIP calls are suffixed with a #.

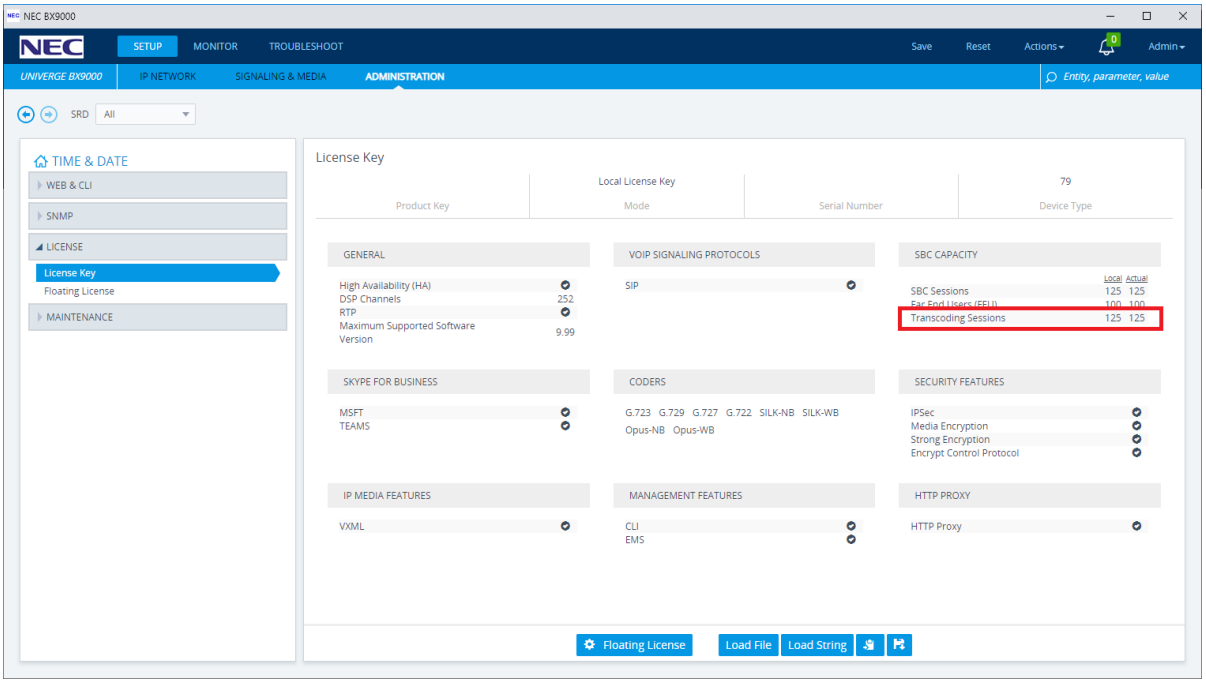


Configure Coder Transcoding (Optional)

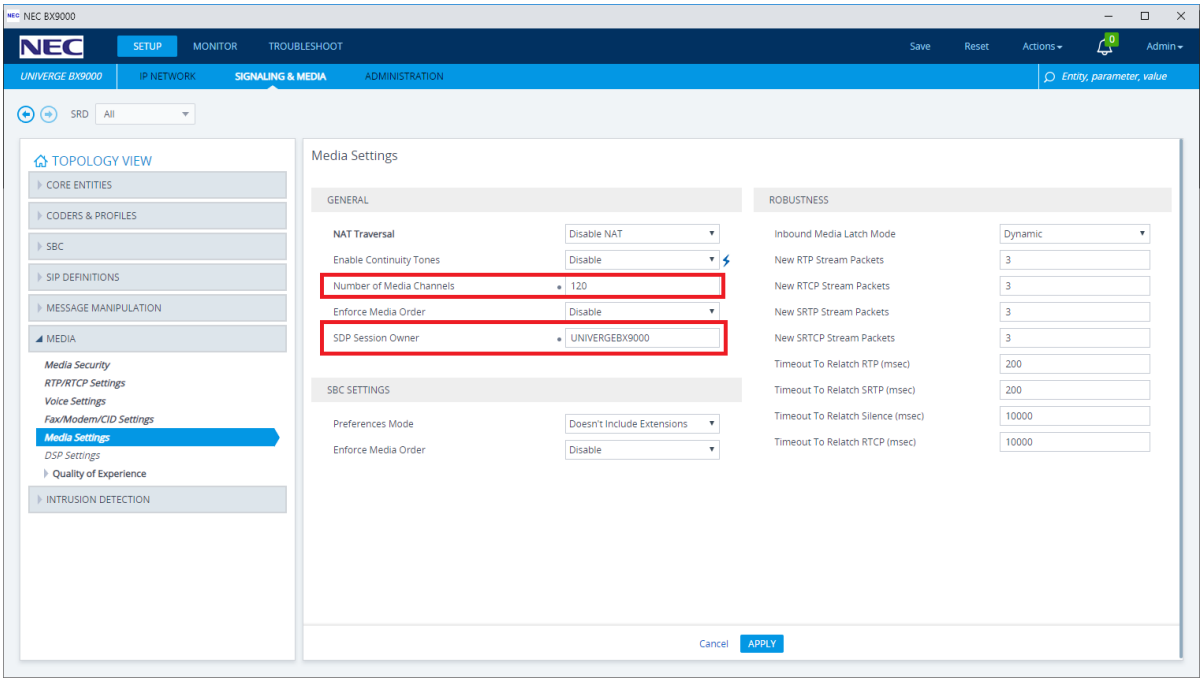
The SV9100 does not support SILK NB or SILK WB codecs. These codecs provide good properties for high latency connections, providing resiliency for lost or delayed RTP packets. The SBC is capable of transcoding calls. This is feature requires hardware DSPs for the BX800 device, or virtual DSPs which are a licensed feature of the BX9000.

This example is based on the BX9000. Transcoding on the BX9000 also requires additional vCPU resources. Please see Release Notes for more information.

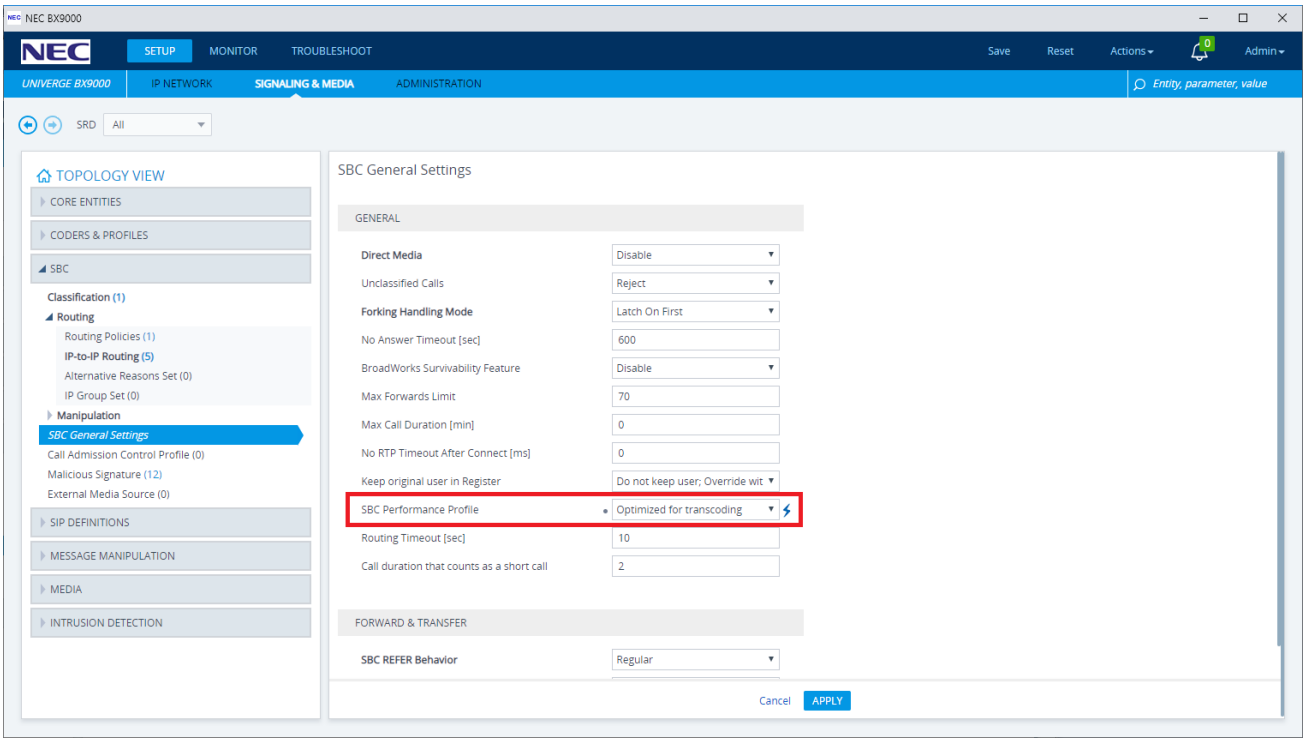
1. Ensure that you have a license key for Transcoding and the codecs are supported in *SETUP > ADMINISTRATION > LICENSE > License Key*.



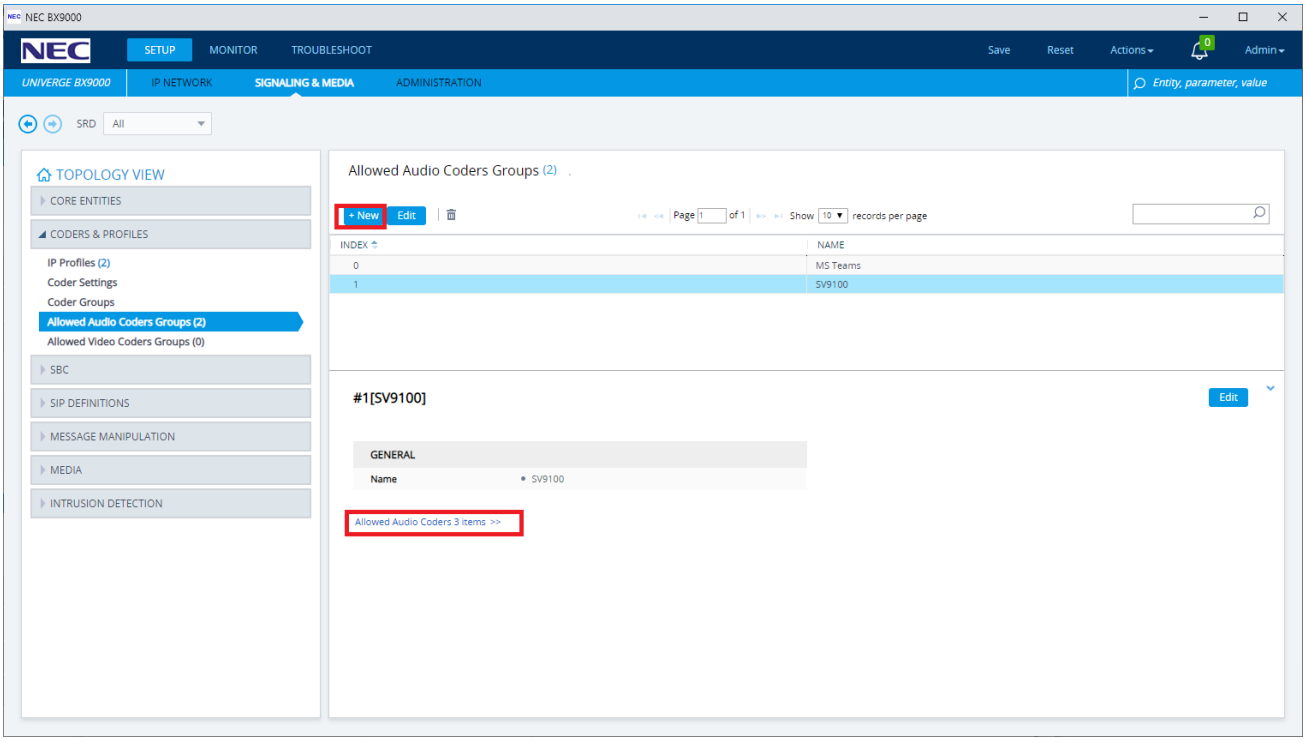
2. Enable the number of Media Channels in *SETUP > SIGNALING & MEDIA > MEDIA > Media Settings.* Also check that the SDP Session Owner does not contain any illegal characters (space).



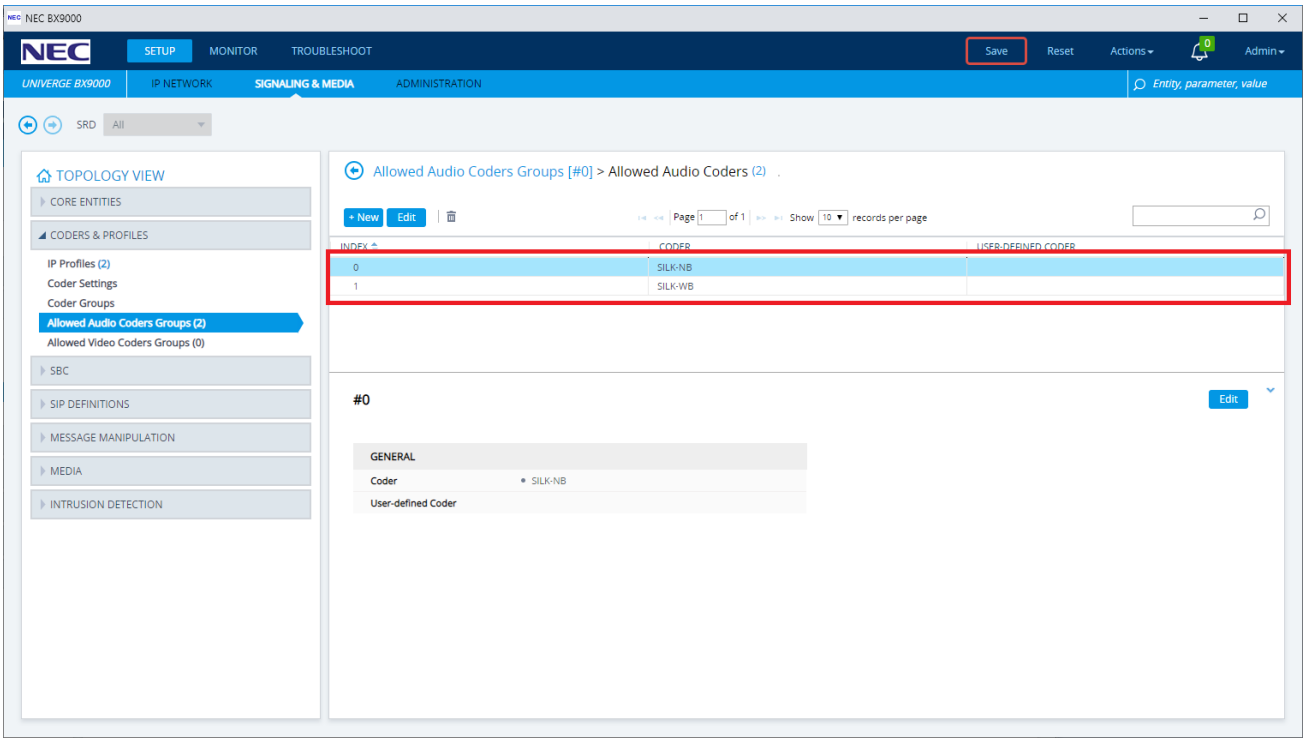
3. Enable Transcoding support in *SETUP > SIGNALING & MEDIA > SBC > SBC General Settings.*



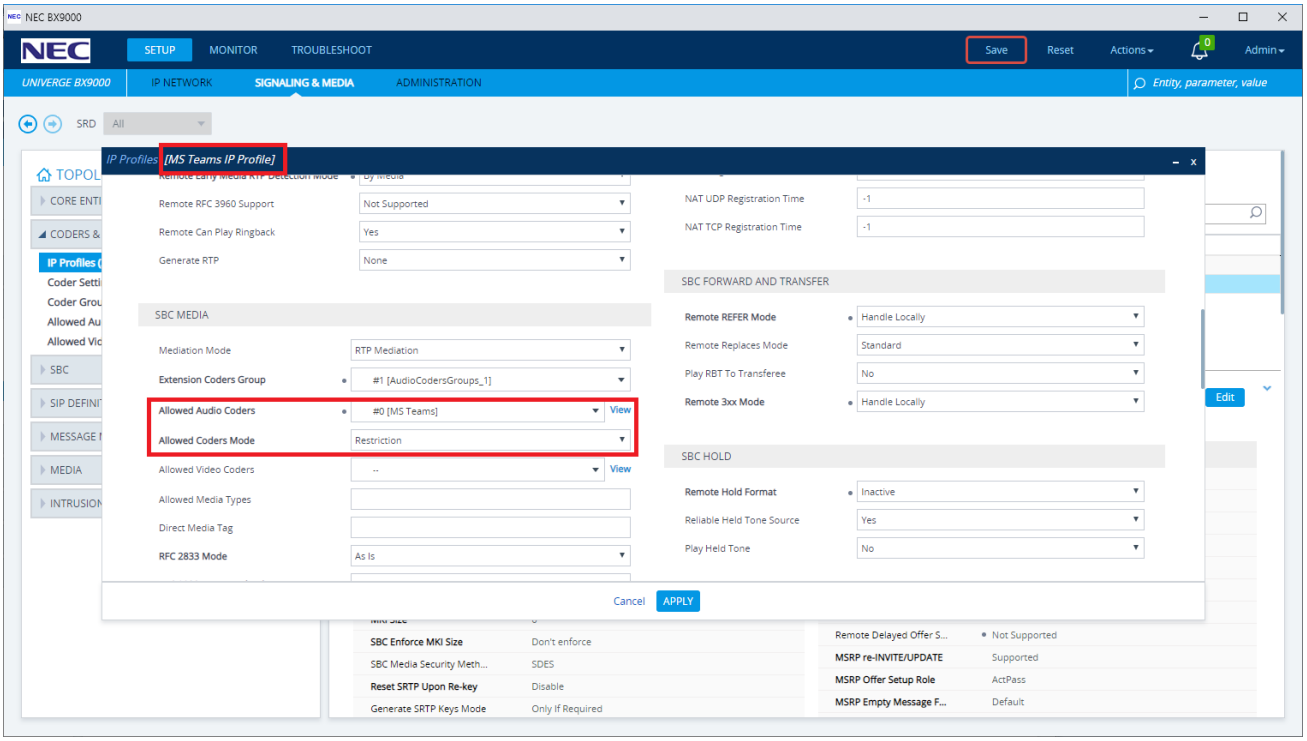
4. Create an 'Allowed' coder group for MS Teams in *SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Allowed Audio Coders Groups.* Open the child table.



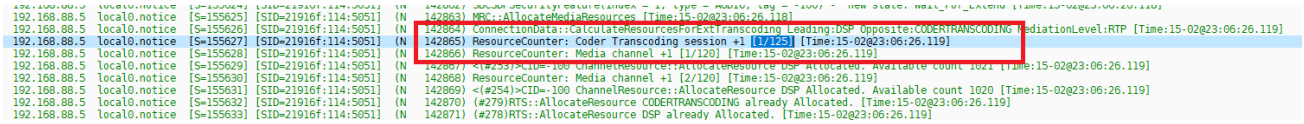
5. In the child table add the restricted codecs.



6. Associate the restricted codecs list with the MS Teams IP Profile in *SETUP > SIGNALING & MEDIA . CODERS & PROFILES > IP Profiles*.



7. Verify the transcoding function is functioning. You can check this in the syslog debug of the BX SBC.



Tested Call Scenarios

Below is a list of tested call scenarios with SV9100 and MS Teams tie-line using Direct Routing.

After each test the trunk resources should be released.

Index	Category	Description	Pass / Fail	Remarks
0	Basic Call Function	Make a call from SV9100 PBX User to MS Teams User	Pass	Incoming call may be displayed in MS Teams client as +442XX. It is possible to call back because SBC manipulates dialled number.
1	Basic Call Function	Make a call from MS Teams client to SV9100 PBX User	Pass	
2	Basic Call Function	Hold call from SV9100 > MS Teams using Teams Client. Recover caller.	Pass	
3	Basic Call Function	Hold call from SV9100 > MS Teams using SV9100 MLT. Recover caller.	Pass	
4	Outgoing Calls – PSTN	Outgoing call from MS Teams Client to SV9100 Trunk via tie-line	Pass	
5	Incoming Calls	DDI Routed from SV9100 Trunk to MS Teams User (22-11)	Pass	Routing of DDI's to F-Route numbers assigned to MS Teams users in target 1 of the DDI translation table is the only supported method of routing DDI's to MS Teams users. MS Teams users cannot be members of other SV9100 routing methods such as incoming ring groups, department groups, etc.
6	Incoming Calls	DDI Routed from SV9100 Trunk to MS Teams Auto Attendant	Pass	Call is answered and DTMF dial options OK, plus also speech analysis.
7	Incoming Calls	DDI Routed from SV9100 Trunk to MS Teams Call Queue	Pass	Call is routed to queue group, receives queue hold music and deliver to agent OK.
8	Call Transfer - PSTN	DDI call to SV9100 MLT > Blind Transfer to MS Teams	Pass	CLIP depends on values set in *Flexible CLI + CLI Pass through*. Either SV9100 MLT or incoming call CLI.
9	Call Transfer - PSTN	DDI call to SV9100 MLT > Consult Transfer to MS Teams User	Pass	CLIP depends on values set in *Flexible CLI + CLI Pass through*. Either SV9100 MLT or incoming call CLI.
10	Call Transfer - PSTN	DDI call to SV9100 MLT > Blind Transfer to MS Teams User – No answer from MS Teams	Pass	Transfer recall to SV9100 station. Missed call notification on MS Teams. CLIP depends on values set in *Flexible CLI + CLI Pass through*. Either SV9100 MLT or incoming call CLI.
11	Call Transfer – PSTN	DDI call from SV9100 Trunk – DDI to MS Teams user, Blind transfer back to SV9100 MLT.	Pass	During the transfer 2 trunks are occupied. CLIP passed by MS Teams is the original incoming caller CLI.
12	Call Transfer – PSTN	DDI call from SV9100 Trunk – DDI to MS Teams user, Consult transfer back to SV9100 MLT.	Pass	During the transfer 2 trunks are occupied. CLIP passed by MS Teams is the MS Teams User PSTN Number.
13	Call Transfer	Call from SV9100 MLT > Teams User. Blind transfer back to SV9100 (different) user.	Pass	During the transfer 2 trunks are occupied.

14	Call Transfer	Call from SV9100 MLT > Teams User. Consult transfer back to SV9100 (different) user.	Pass	During the transfer 2 trunks are occupied.
15	Call Transfer	Call from SV9100 MLT > Teams User. Consult transfer back to SV9100 but cancel call during transfer.	Pass	During the consult 2 trunks are occupied.
16	Call Forward	Immediate Call forward SV9100 MLT to MS Teams User	FAIL	Under investigation
17	Call Forward	Call forward from MS Teams User on Immediate to SV9100 MLT	Pass	
18	Call Forward	Call forward from MS Teams User on No Answer to SV9100 MLT	Pass	
19	Voicemail - PSTN	DDI call to MS Teams user with B/NA to voicemail set	Pass	Call is redirected and CLI passed to VM
20	Voicemail	Call from SV9100 MLT to Teams User with B/NA to voicemail set	Pass	Call is redirected to VM.
21	Conference	SV9100 MLT setup conference by adding MS Teams user	Pass	MS Teams user is added to conference call
22	Dial-Through	Dial through the SV9100 to PSTN trunk	Pass	Call transits the SV9100. Requires Tie-Line COS 20-14-02 and 20-14-03 enabled. SBC is responsible for adding trunk access prefix
23	Dial-Through	Dial through the SV9100 to PSTN trunk and access remote IVR/AA system. Check that DTMF digits are received and analysed OK	Pass	Digits 0-9, # and * OK.
24	Dial-Through	Send CLI through transit trunks	Pass	Supported if 14-01-24 is enabled and dependent upon support from PSTN network.