Connecting NEC UNIVERGE® SV9100/SL2100 with Calls2Teams using NEC BX Series SBC

Version History

Version	Date	Notes and Changes
1.0	19/07/2022	1. Initial release of integration

Contents

Purpose of this document:

This article describes the UNIVERGE SV9100/ SL2100 Series integration with Qunifi Ltd.'s Call2Teams for Microsoft® Teams service and provides a guideline for how a SIP device can be configured on a SV9100 Series communications environment to inter-operate with a Call2Teams user (SL2100 screenshot will differ from the SV9100 but functionality is similar). 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 Qunifi Ltd.'s Calls2Teams environment and an NEC SV9100. 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 12.10.52
SV9100 CP20 PC Pro 12.12.53
SL2100 Main software 4.20.02
SL2100 PC Pro 4.20.02
NEC BX9000 7.20A.258.459

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

Calls2Teams description

Call2Teams is a companion service to Office 365 that allows customers to use their existing NEC communications platform with Microsoft Teams. Once setup is complete, customers with a Call2Teams service and Office 365 will be able to use the O365 phone system add-on to make and receive calls through their Microsoft Teams client using their organization's UNIVERGE SV9100 phone service.

Prerequisites

The following prerequisites are necessary in order to achieve integration between Calls2Teams and NEC's SV9100.

Qunifi Calls2Teams

Sufficient Calls2Teams user licenses for all Teams users which require integration to the NEC SV9100.

Calls2teams licenses are purchased direct from Qunifi or one of Qunifi's partners.

Microsoft Office 365 Subscription

Microsoft package	Requirements
Microsoft 365 Business Basic, Standard, Premium	Common Area Phone license

Microsoft or Office E1 and/or E3	Phone System license or Common Area Phone license
Microsoft or Office E5	E5 includes the Phone System license

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
- 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 3rd party SIP extension capability of the SV9100. For each Calls2Teams user the following is required;

- 3rd Party IP Phone license (BE114054) – One license is required for each Calls2Teams client
- System Capacity license (BE114042) – Required for additional system capacity
- IPLE VoIP gateway card (BE113281) – Required for DSP channels

SL2100

- 3rd Party IP Phone license (EU909388 / BE116746) – One license is required for each Calls2Teams client
- VOIP expansion license (BE120530) – Adds 8 VOIP channels to built-in VOIP
- VoIP expansion card (BE116500) – Required for 17 VOIP channels or more

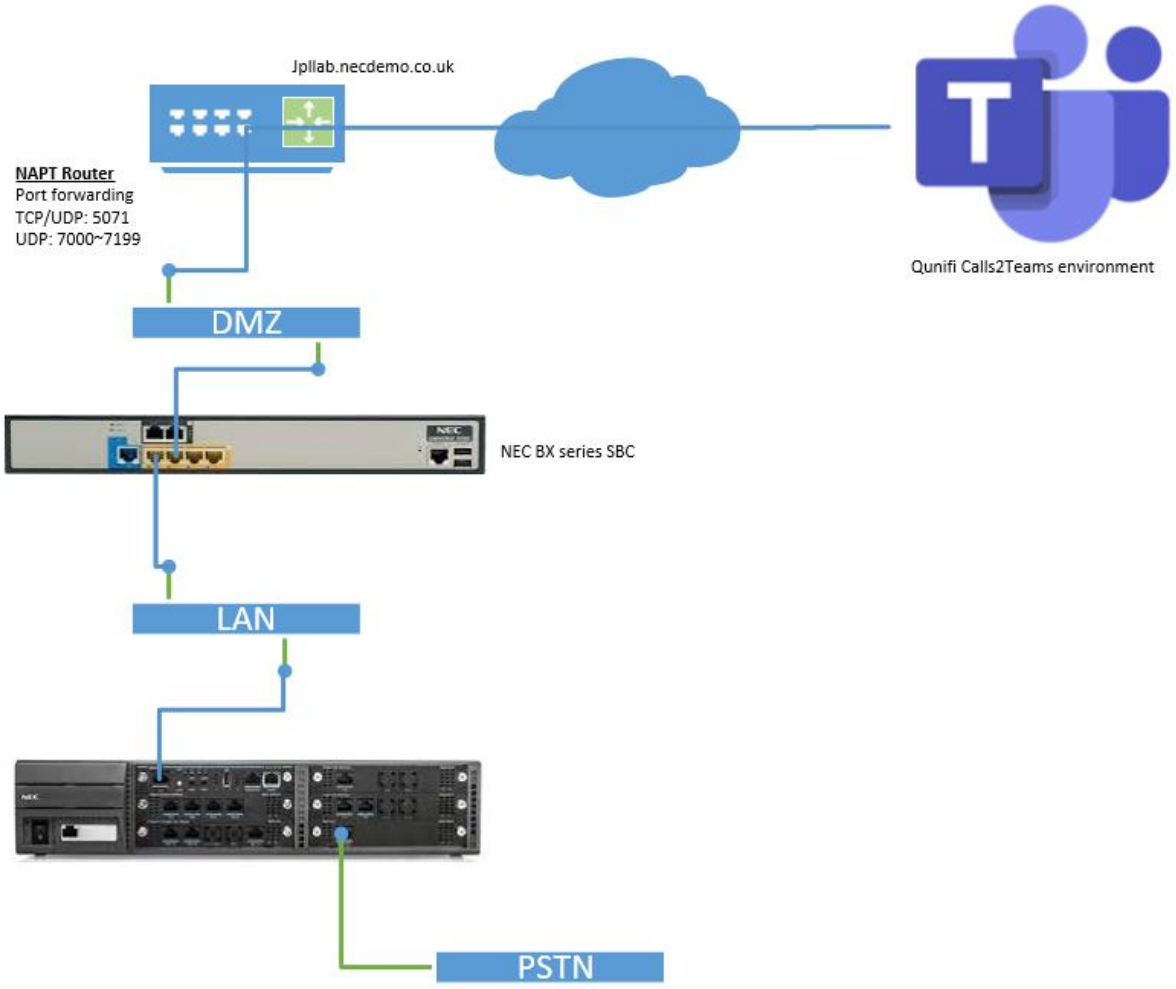
Network Infrastructure

The connection to Calls2Teams is supported using UDP, TCP, and TLS. This means the following networking requirements must be met.

- Fixed public IP Address for WAN connection
- Firewall configuration supporting port forwarding for SIP connectivity – See connectivity diagram

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 JPLLAB.necdemo.co.uk to the public IP address of the customer router. The customer router then forwards connections from port TCP/UDP:5071 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.

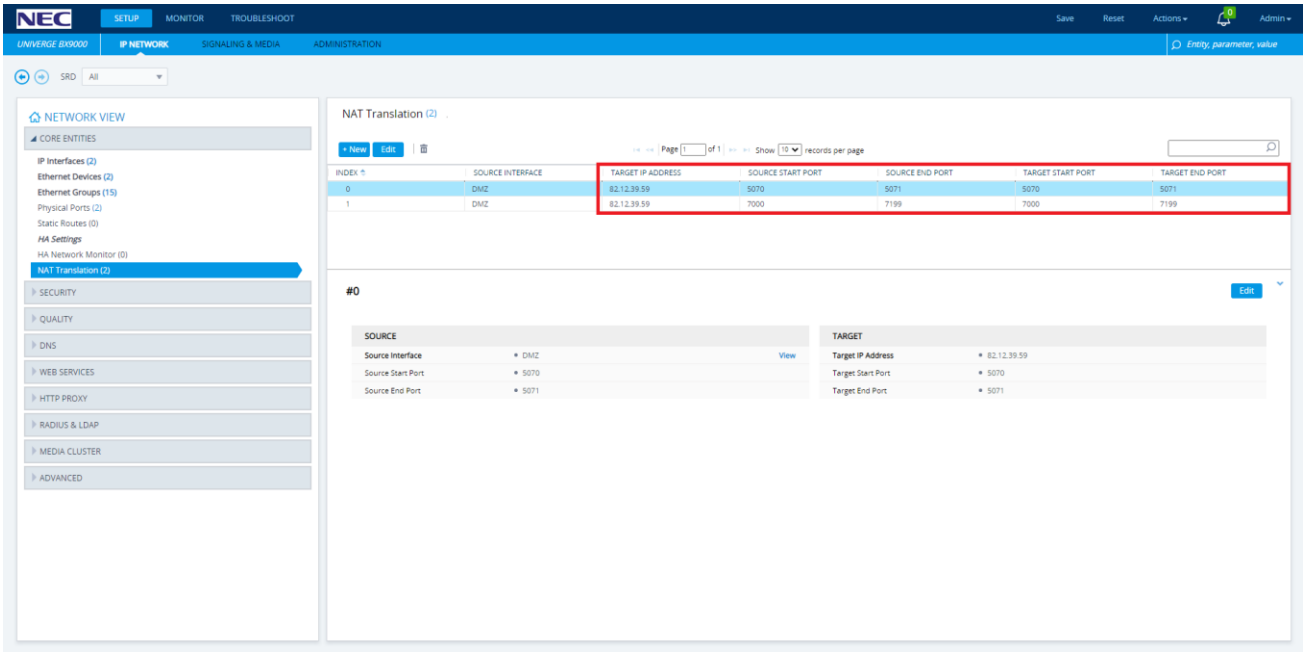
Configure IP Interfaces and NAT Traversal

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.

Signalling – TCP/UDP:5071
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.

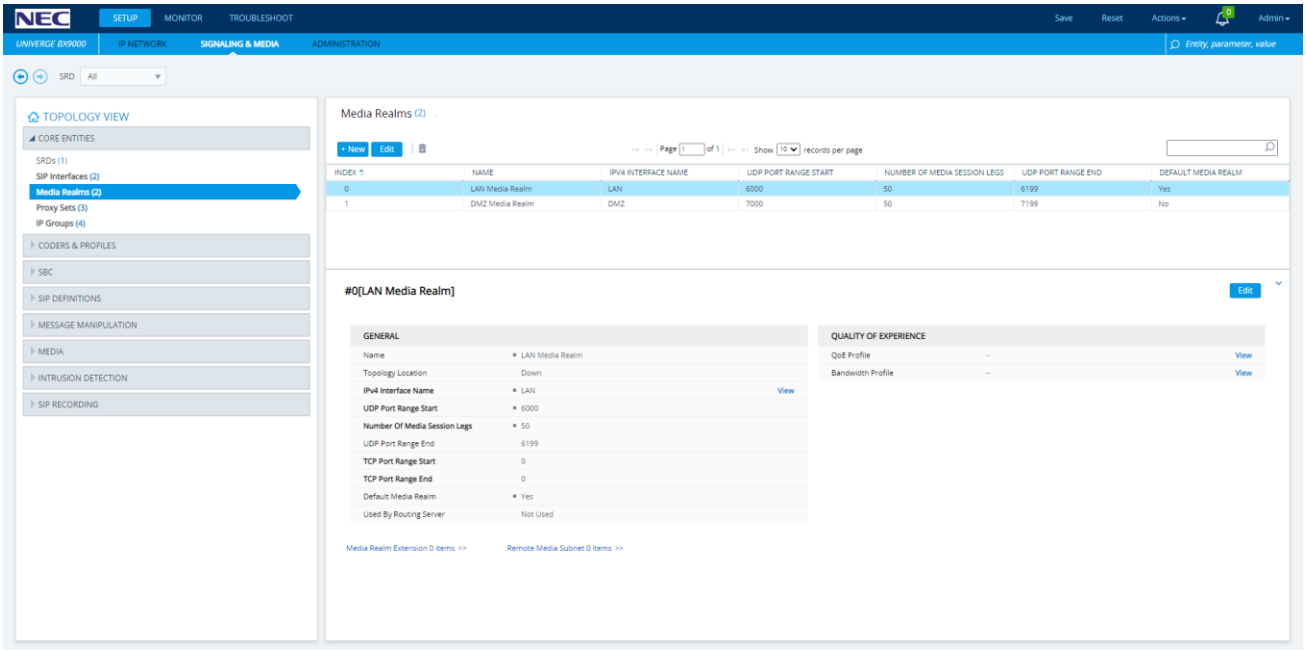
NAT Translation is configured to ensure that SIP Signalling includes the Public IP address of the customer site instead of the internal private IP address.

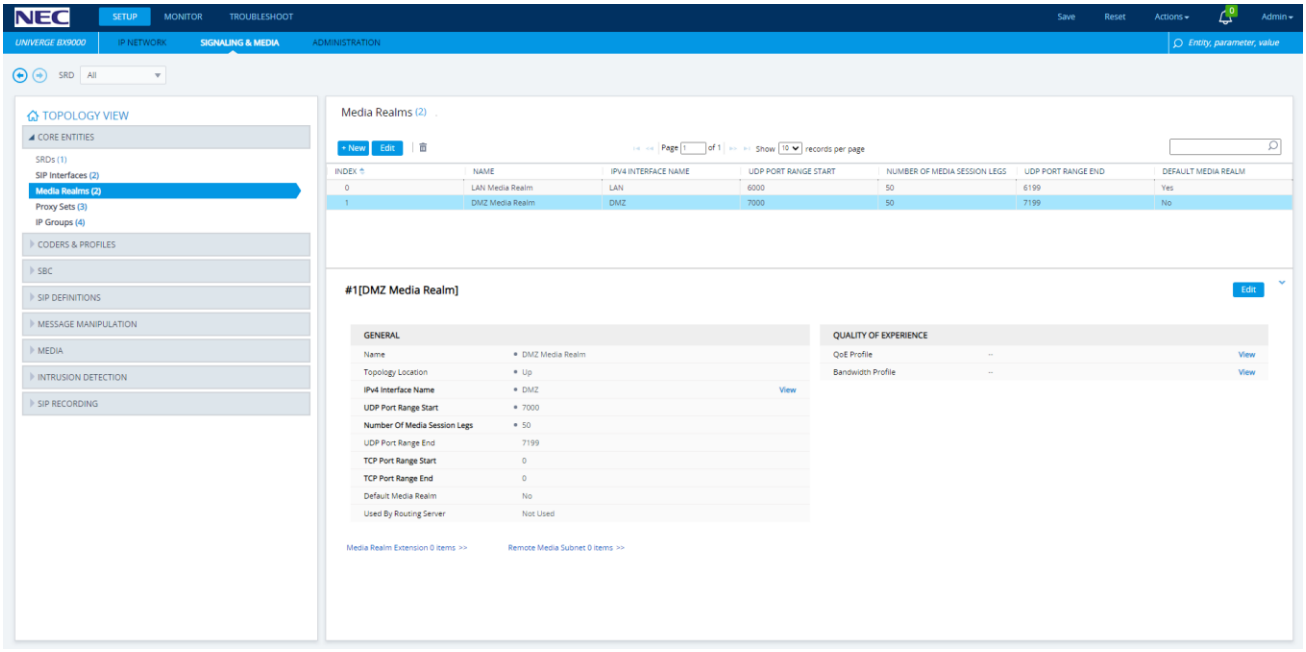


Configure Media Realms

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



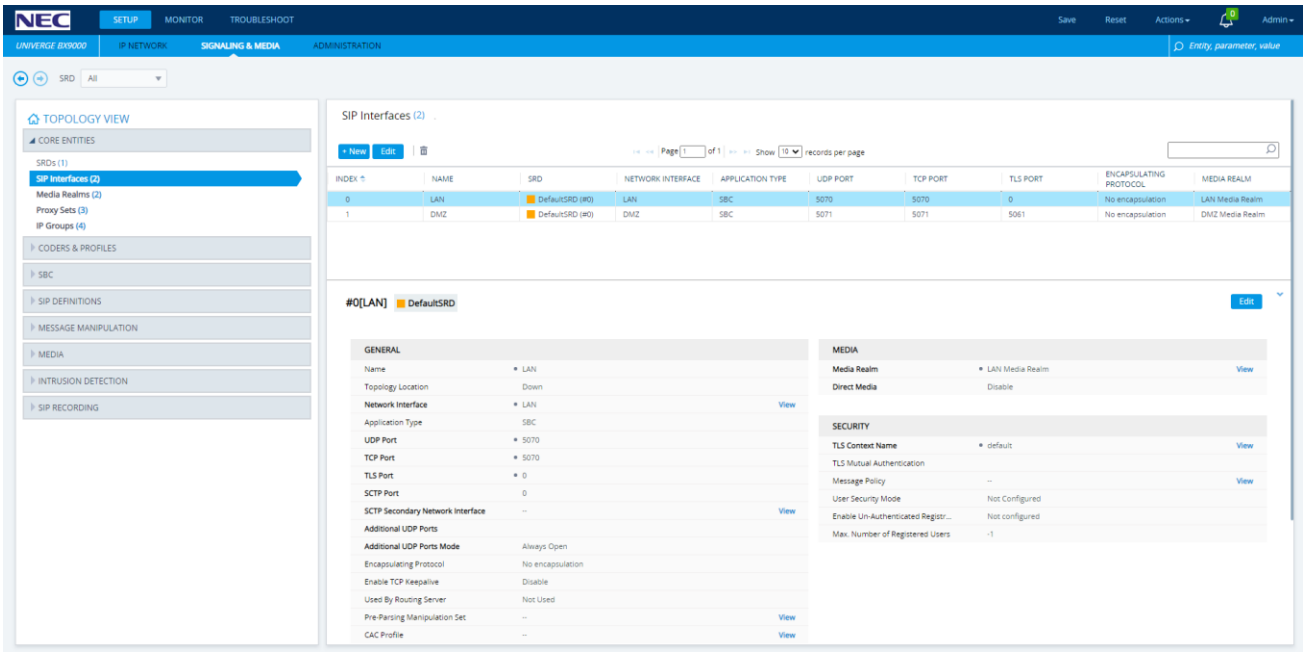


Configure SIP Interfaces

This section shows how to configure the SIP listening interfaces for the SBC. 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*.

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 Qunifi Calls2Teams.



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	5070	5070	0	Disable	500	LAN Media Realm	-	-
WAN SIP Interface	WAN Interface	SBC	5071	0	0	Disable	0	WAN Media Realm	-	-

Configure Proxy Sets and Proxy Addresses

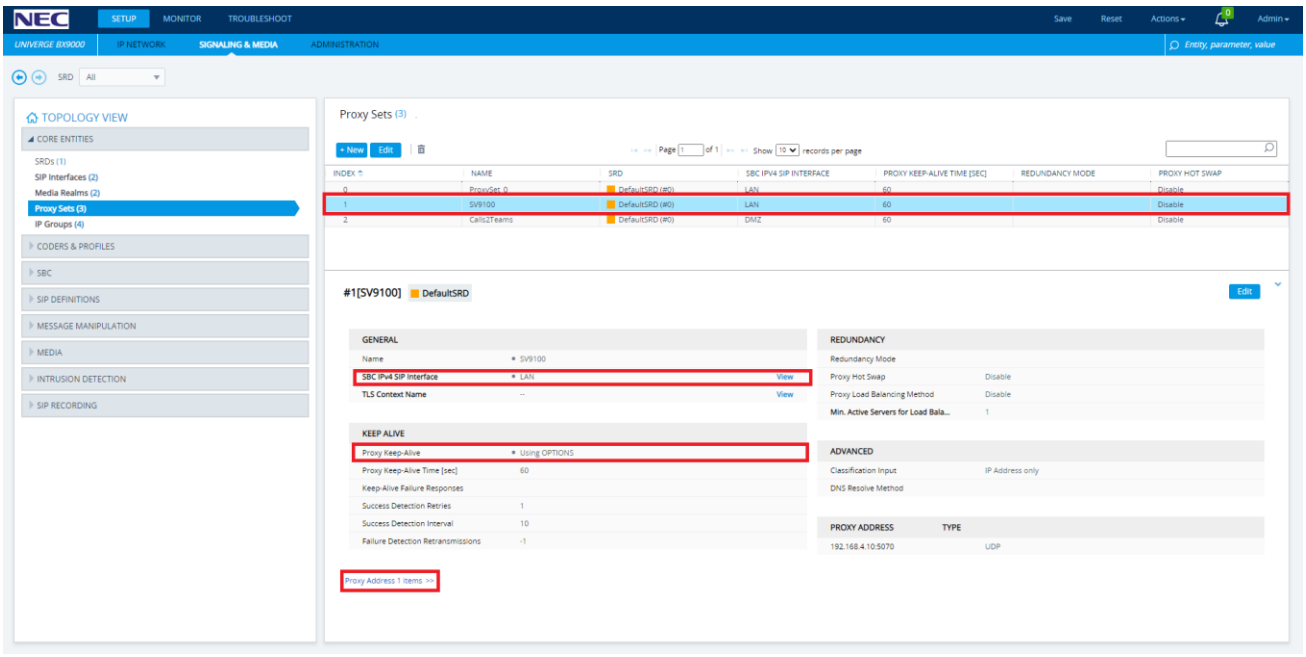
The Proxy set defines a service connected to the SBC, the parameters, ports hostnames or IP addresses which are used to communicate with this service.

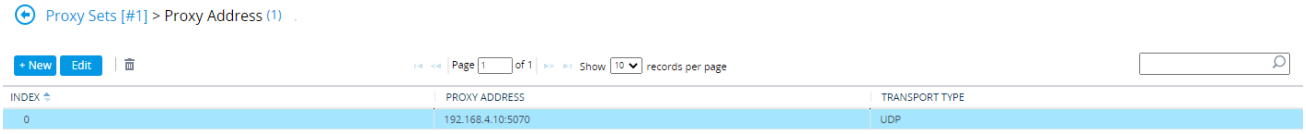
Qunifi Calls2Teams provides 2 redundant SBC's for resiliency. These can be found in the Calls2Teams admin portal. In this example the following SBCs are assigned to the service: 40.69.2.153:6002 & 20.126.150.164:6002

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

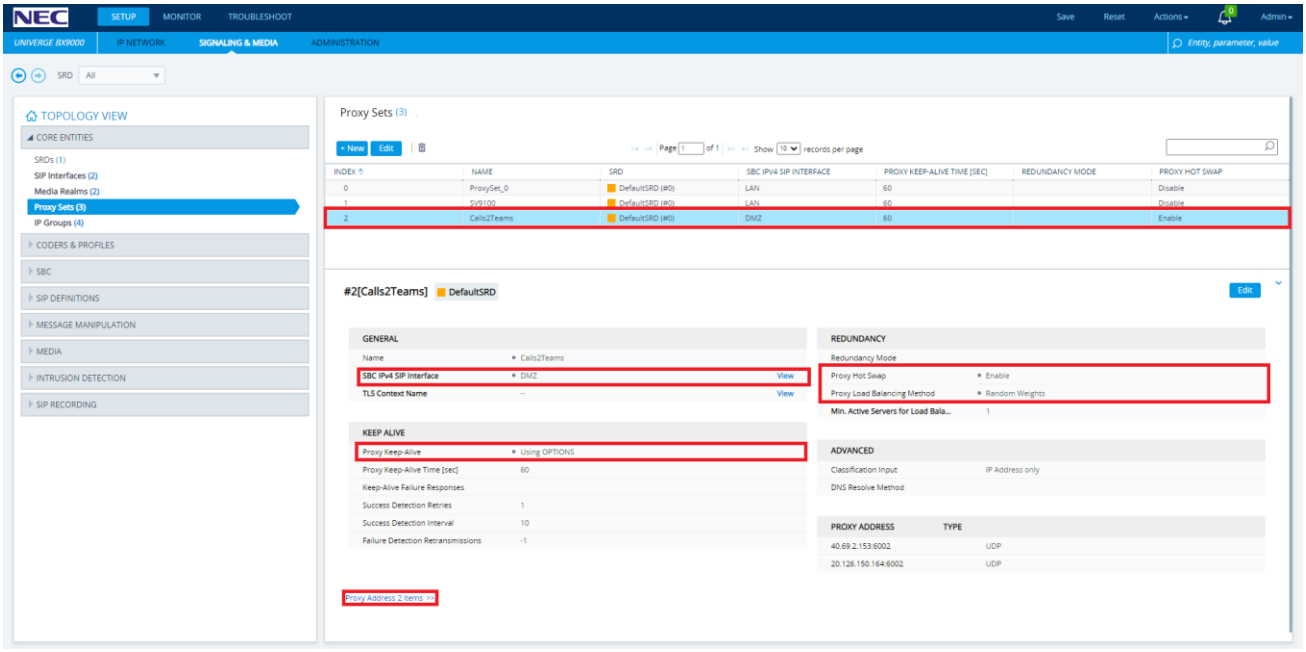
In this example the default 3rd party SIP extension port of 5070 is used on the SV9100. If this port is changed reflect the value from command 84-20-01 in place of 5070.

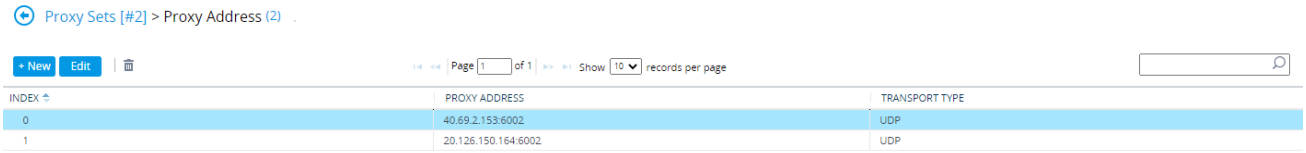
1. Configure a Proxy Set for the SV9100. Ensure that OPTIONS method is selected for the Proxy Keep-Alive method and that the LAN SIP Interface is used. Using the Proxy Address child table (link at bottom of the page) configure the IP:Port of the SV9100.





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 Calls2Teams.

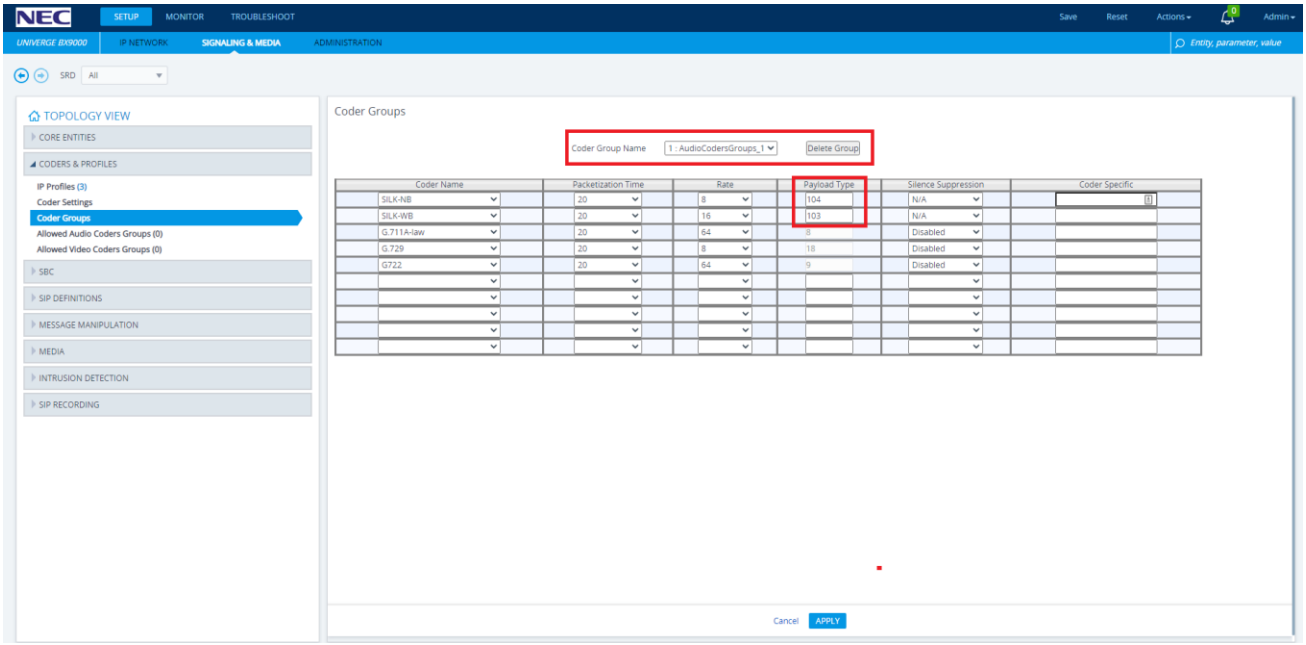




Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	40.69.2.153:6002	UDP	1	1
1	20.126.150.164:6002	UDP	2	1

Configure Coder Groups

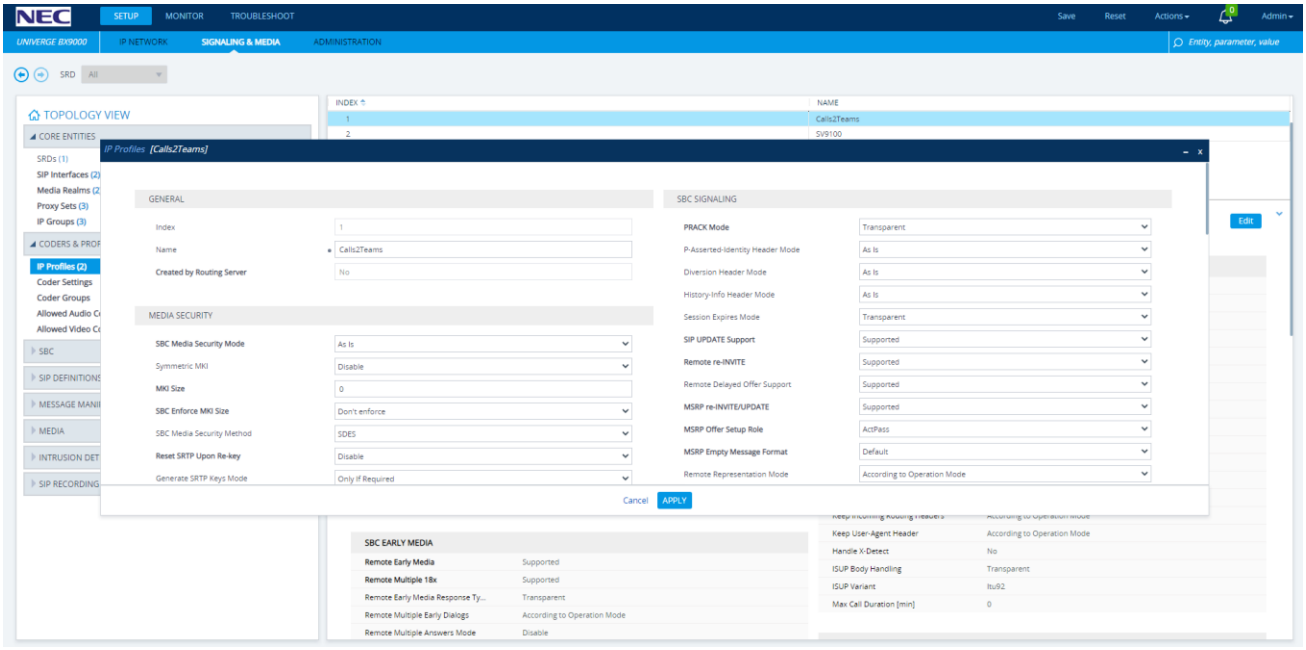
This section describes how to configure coders. Calls2Teams supports a wide selection of codes including SILK NB and WB as well as G.711. To create the coder group navigate to *SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Coder Groups*. Enable the codecs which you would like to use towards MS Teams. In order to use SILK NB or WB transcoding is required and is detailed later in this documentation. To use G.711, add only G.711 A-law to the coders list.



Configure the IP Profile for Calls2Teams

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.

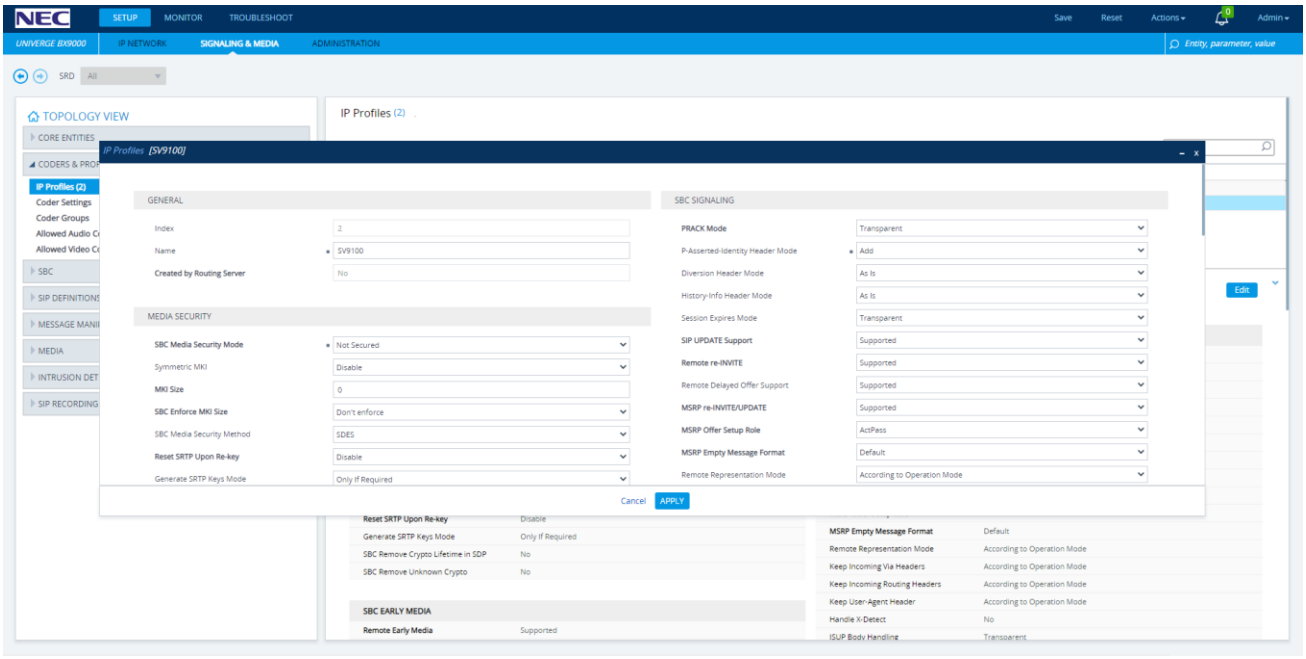
1. Open the IP Profiles table in *SETUP > SIGNALING & MEDIA > CODERS & PROFILES > IP Profiles.* Use the **+New** button to add a new IP Profile.



Name	Parameter
General	
Name	Calls2Teams (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	As is
SBC Media	
Extension Coders Group	AudioCodersGroups_1
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.

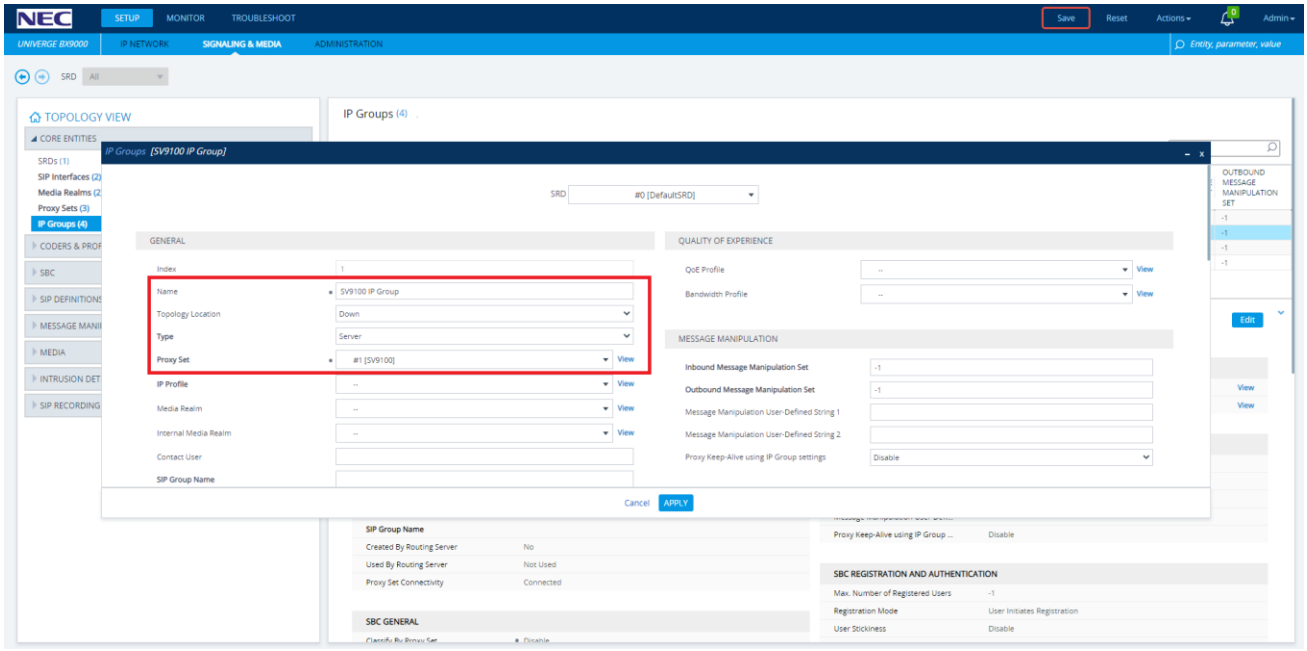


Name	Parameter
General	
Name	SV9100 (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	Not Secured
SBC Signaling	
P-Asserted-Identity Mode	Add
All other parameters can be left unchanged at their default values.	

Configure IP Groups

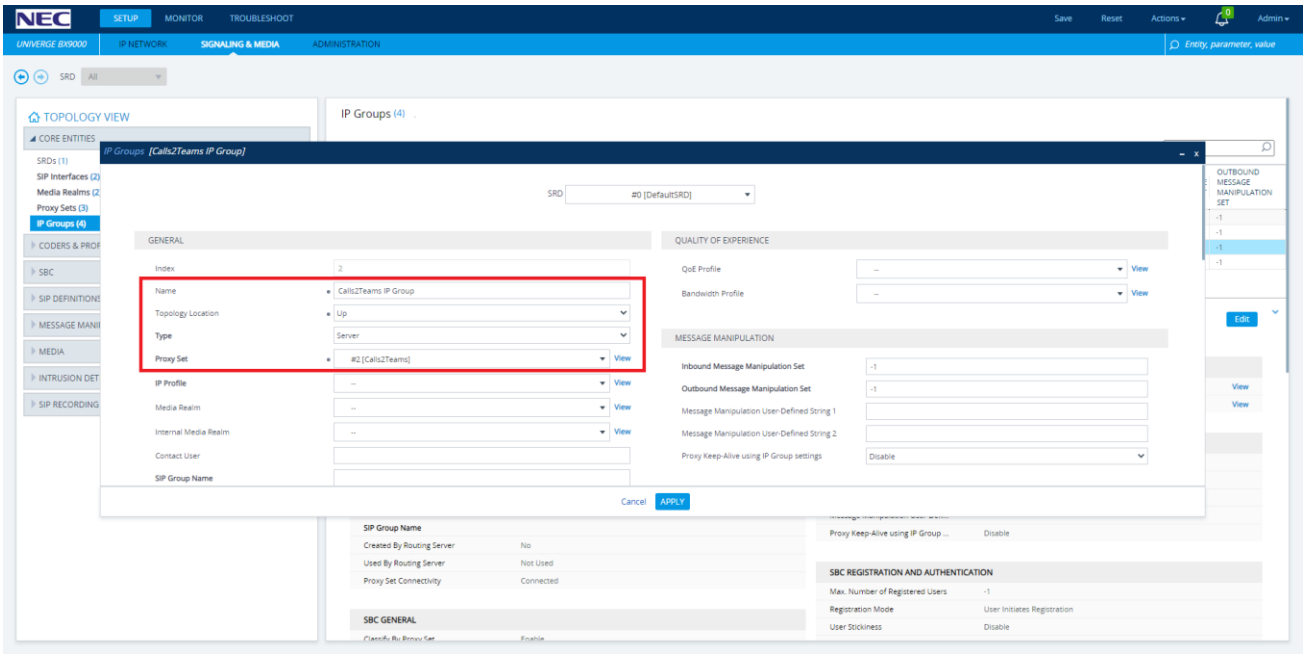
This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP-PBX or SIP Trunk) or it can be a group of users. For servers, the IP Group is typically used to define the server's IP address by associating 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.



Name	Parameter
General	
Name	SV9100 (arbitrary descriptive name)
Topology Location	Down
Type	Server
Proxy Set	SV9100
SBC General	
Classify By Proxy Set	Enabled

2. Configure an IP Group for MS Teams.



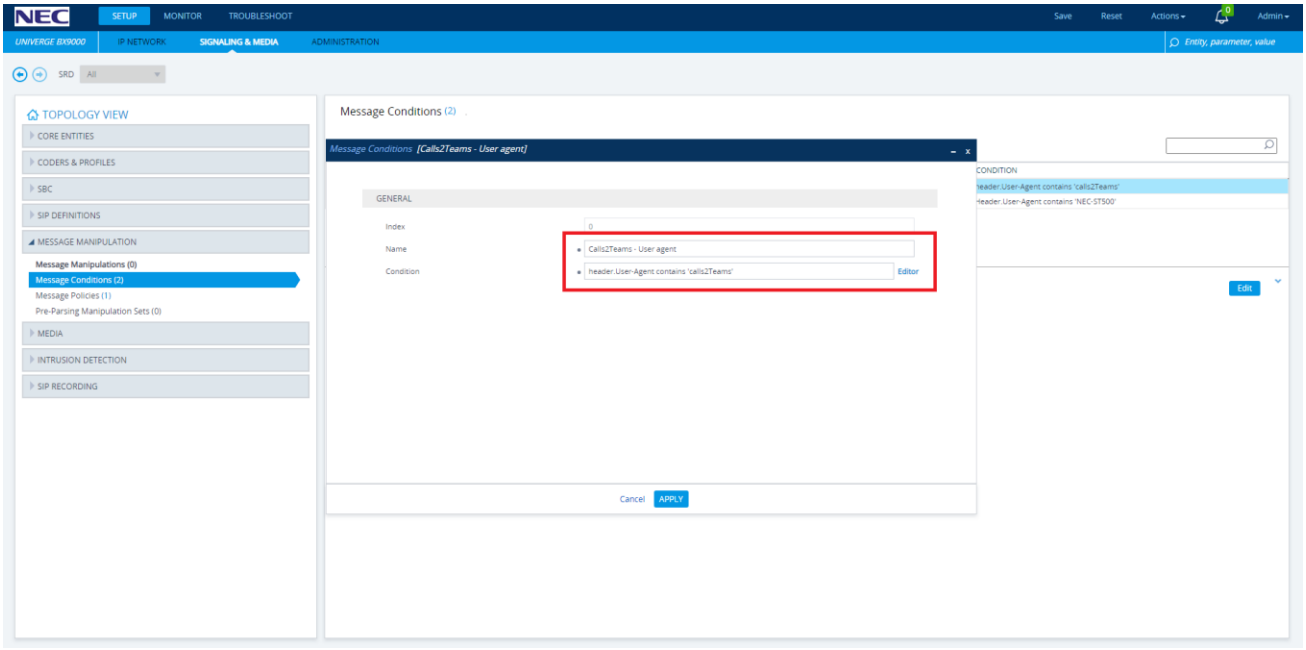
Name	Parameter
General	
Name	MS Teams (arbitrary descriptive name)
Topology Location	Up
Type	Server
Proxy Set	Calls2Teams
SBC General	
Classify By Proxy Set	Enable
All other parameters can be left unchanged at their default values.	

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.

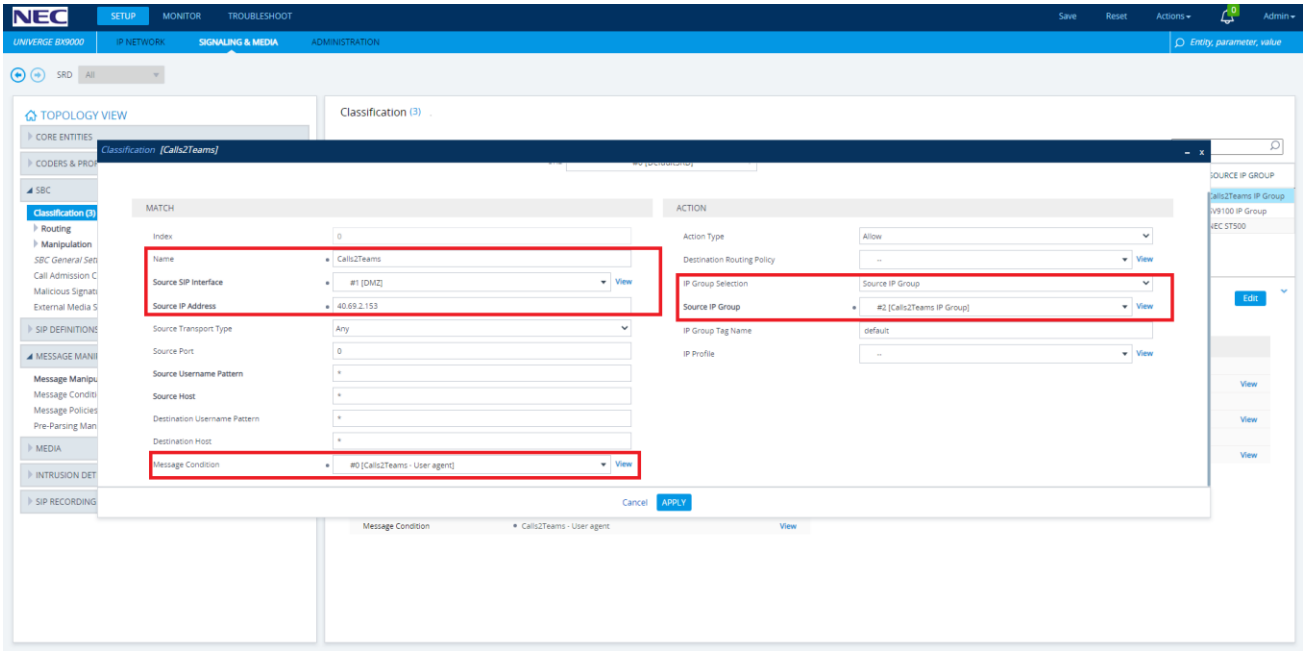
The classification rules are more secure when Message Conditions are included. To create the necessary Classification Rules for Calls2Teams communication;

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



Parameter	Value
Name	Calls2Teams User Agent (arbitrary descriptive name)
Condition	header.User-Agent contains 'calls2Teams'

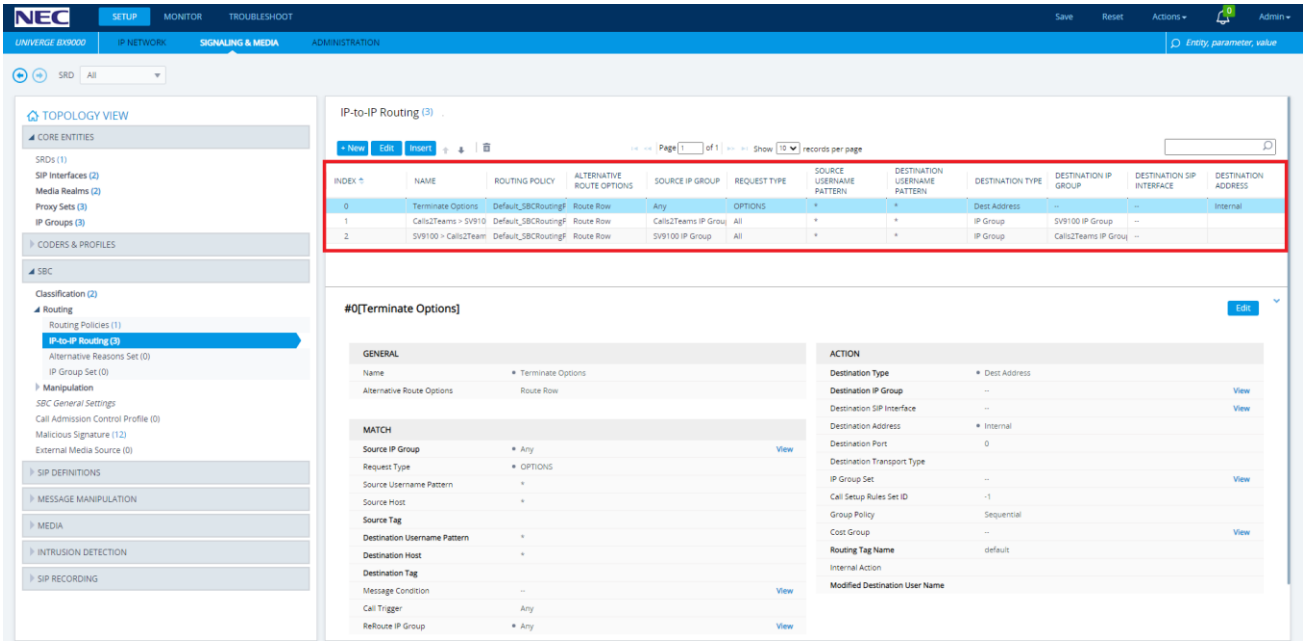
2. Navigate to *SETUP > SIGNALING & MEDIA > SBC > Classification.* Add a new Classification rule for Calls2Teams with the following conditions to allow known traffic to pass SBC security.



Parameter	Value
Name	Calls2Teams (arbitrary descriptive name)
Source SIP Interface	DMZ
Source IP Address	As per Qunifi portal
Message Condition	Calls2Teams User Agent
Action Type	Allow
Source IP Group	Calls2Teams IP Group

Configure IP-to-IP Routing Rules

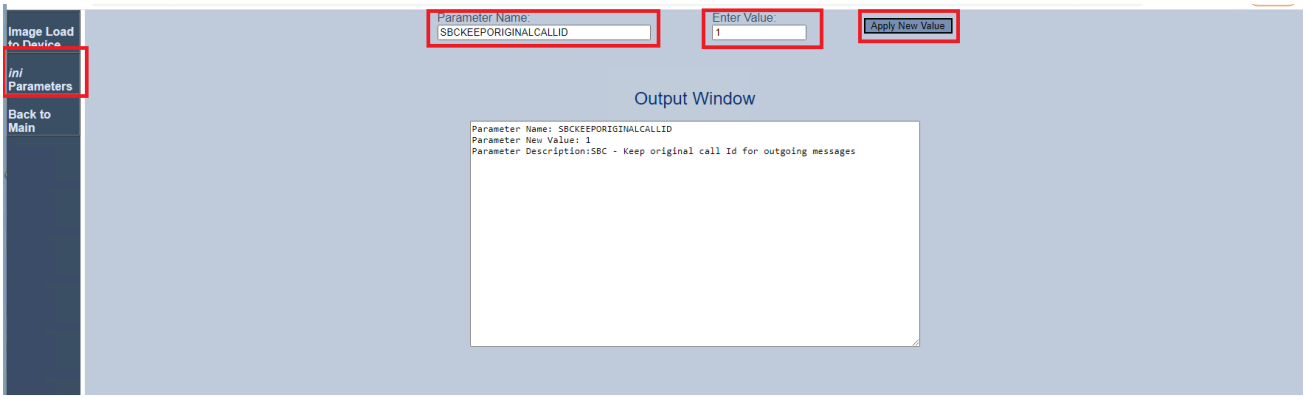
This section describes how to configure the necessary IP-to-IP Routing rules for communication between the SV9100 PBX and MS Teams Cloud PBX. These rules may vary depending on other functions of the SBC. As a minimum the rules below should be added or configured.



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	Calls2Teams > SV9100	Calls2Teams	All	Any	Any	IP Group	SV9100	-	This rule routes SIP messages from Calls2Teams to the SV9100
2	SV9100 > Calls2Teams	SV9100	All	Any	Any	IP Group	Calls2Teams	-	This rule routes SIP messages from the SV9100 to Calls2Teams

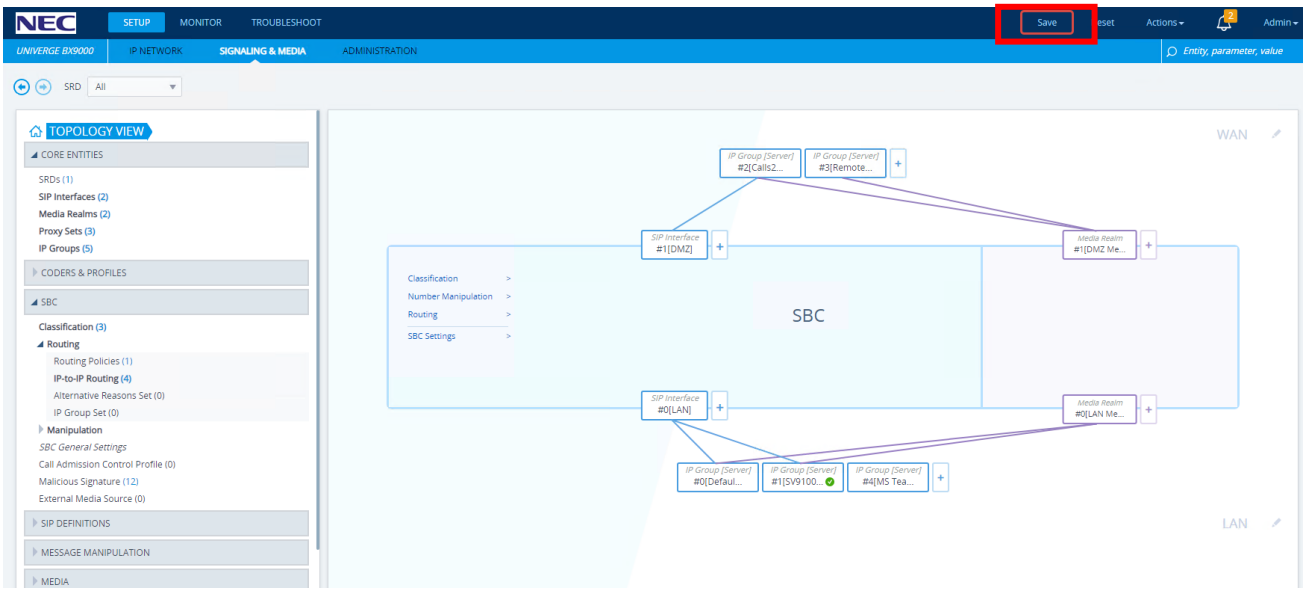
Configure INI Parameters

This section describes how to configure the necessary INI parameters settings. The changes described in this section are made via the SBC's admin page. To access the admin page, browse to http://<IP Address of SBC>/AdminPage. Once logged in, select ini Parameters and input the parameters and click apply new value.



Parameter Name	Value
SBCKeepOriginalCallID	1

Once complete return to the GUI of the SBC and burn the changes using the save icon.

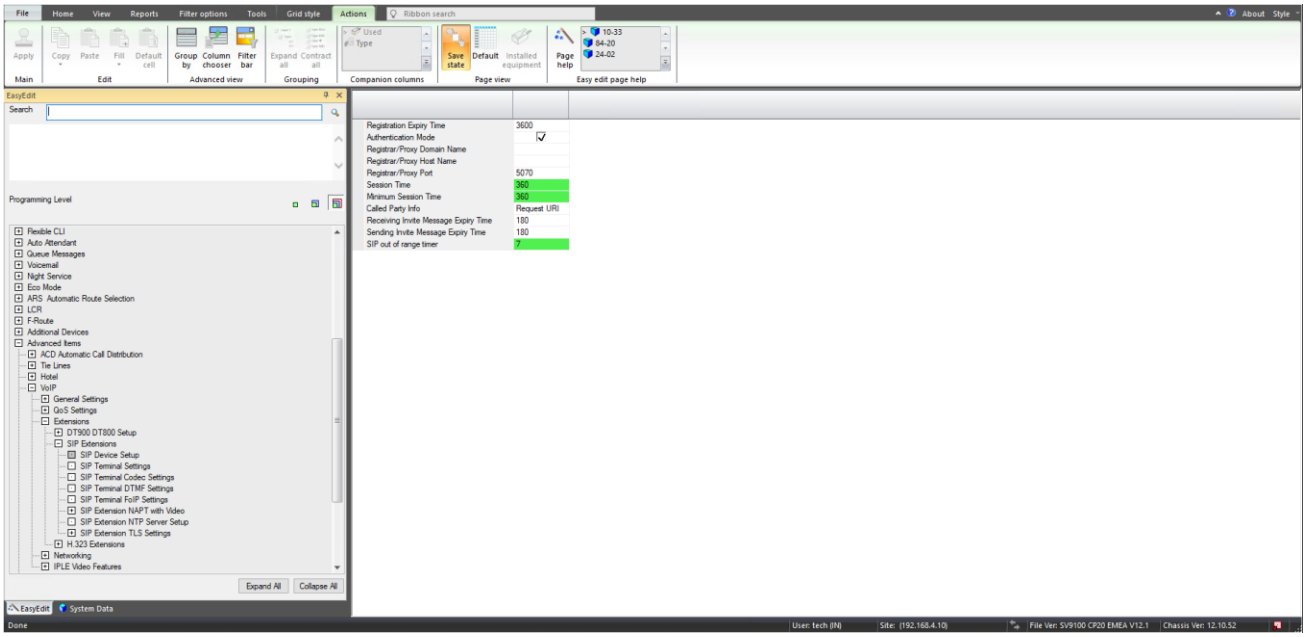


SV9100 Configuration

IP Extension Setup

Using the PCPro application complete the following steps to setup an 3rd party IP extension for each Calls2Teams user.

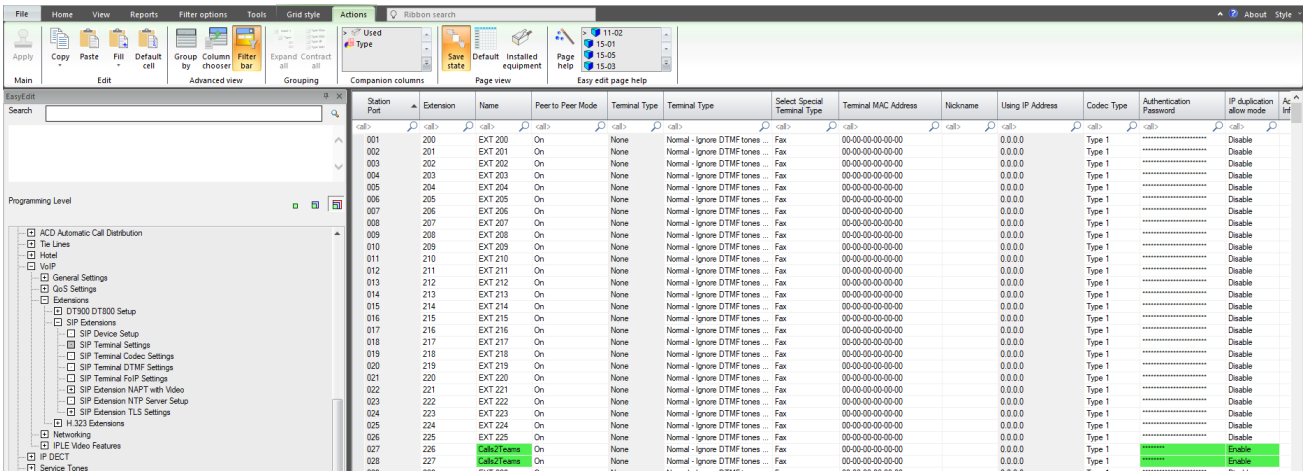
1. Navigate to *Advanced items > VoIP > Extensions > SIP Extensions > SIP device setup*.



2. Configure the recommended standard SIP settings as per your installation requirements

Program Name	Program Number	Input Data	Default Value	Recommended settings
Registration Expiry Time	10-33-01	60 ~ 65535	3600	3600
Authentication Mode	10-33-02	Disabled, Enabled	Enabled	Enabled
Registrar/ Proxy Domain Name	10-33-03	Any	Blank	Blank
Registrar/ Proxy Host Name	10-33-04	Any	Blank	Blank
Registrar/ Proxy Port	84-20-01	1 ~ 65535	5070	5070
Session Time	84-20-02	0 ~ 65535	180	360
Minimum Session Time	84-20-03	0 ~ 65535	180	360
Called Party Info	84-20-04	Request URI, To Header	Request URI	Request URI
Receiving Invite Message Expiry Time	84-20-05	0 ~ 256	180	180
Sending Invite Message Expiry Time	84-20-06	0 ~ 3600	180	180
SIP out of range timer	24-02-15	0 – 64800	4	As per requirements

3. Navigate to *Advanced items > VoIP > Extensions > SIP Extensions > SIP Terminal Settings*.



4. Determine a port range that is unallocated to existing extensions cards or IP terminals and is available for IP extensions.
5. Set an authentication password on the relevant ports. The password should be complex and independent per IP extension.
6. Enabled IP duplication mode on the relevant ports.

Program Name	Program Number	Input Data	Default Value	Recommended settings
Authentication password	15-05-16	Any	N/A	As per requitements
IP duplication mode	15-05-18	Disabled, Enabled	Disabled	Enabled

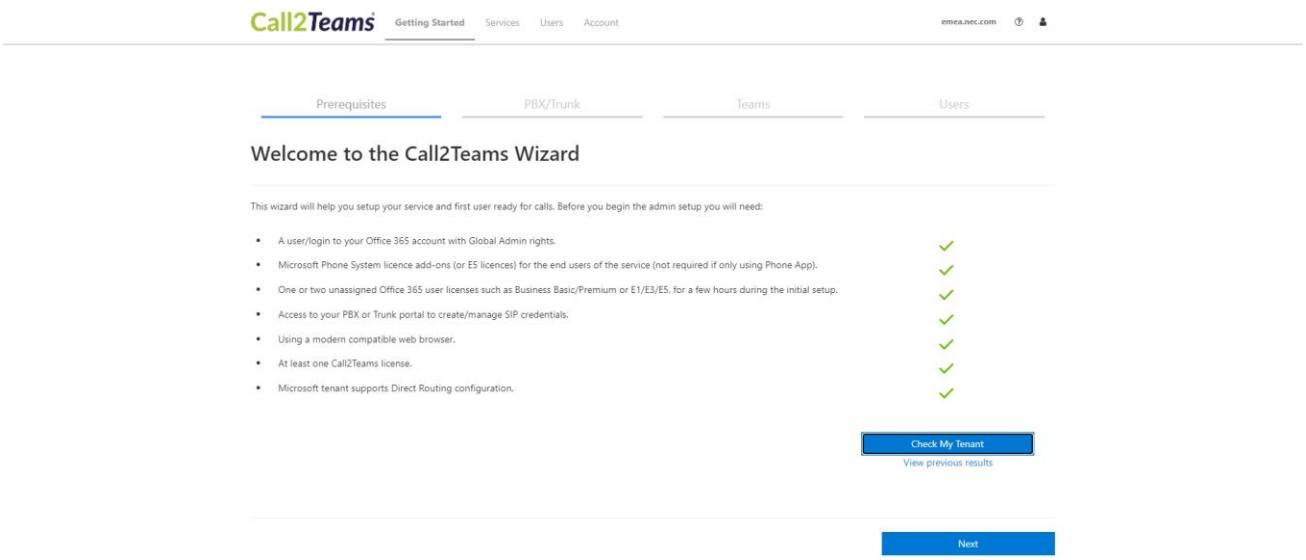
Calls2Teams Configuration

This section describes how to configure the Qunifi Calls2Teams portal for interoperability with the NEC SV9100.

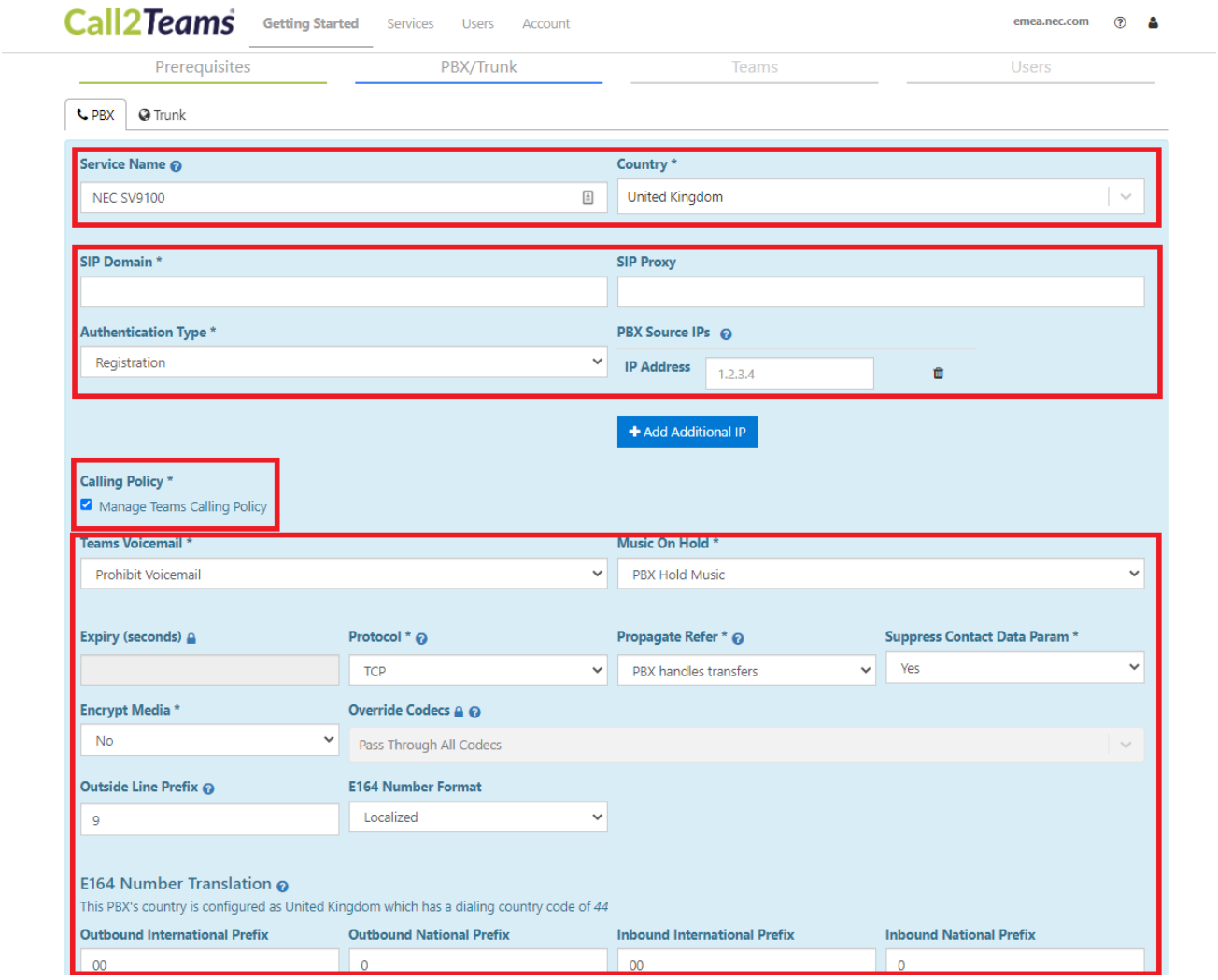
NEC does not provide support for configuration of Calls2Teams components, and the information provided in this section is for guidance only. Care should be taken to review the latest documentation provided by Qunifi.

Calls2Teams Configuration Wizard

1. Click “Check My Tenant” to ensure the detailed Calls2Teams configuration Prerequisites are in place.

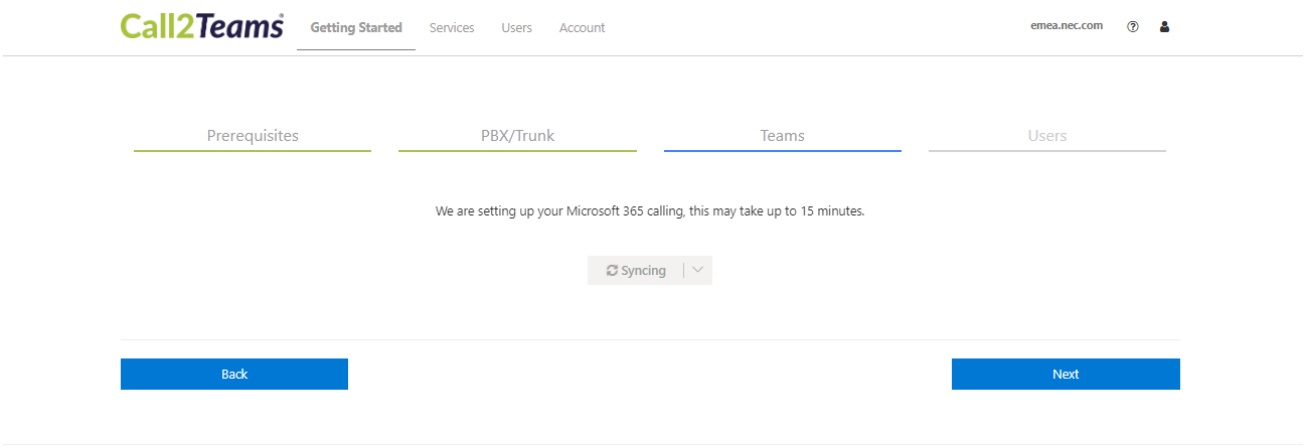


2. Configure the PBX template as required, click save, followed by next.

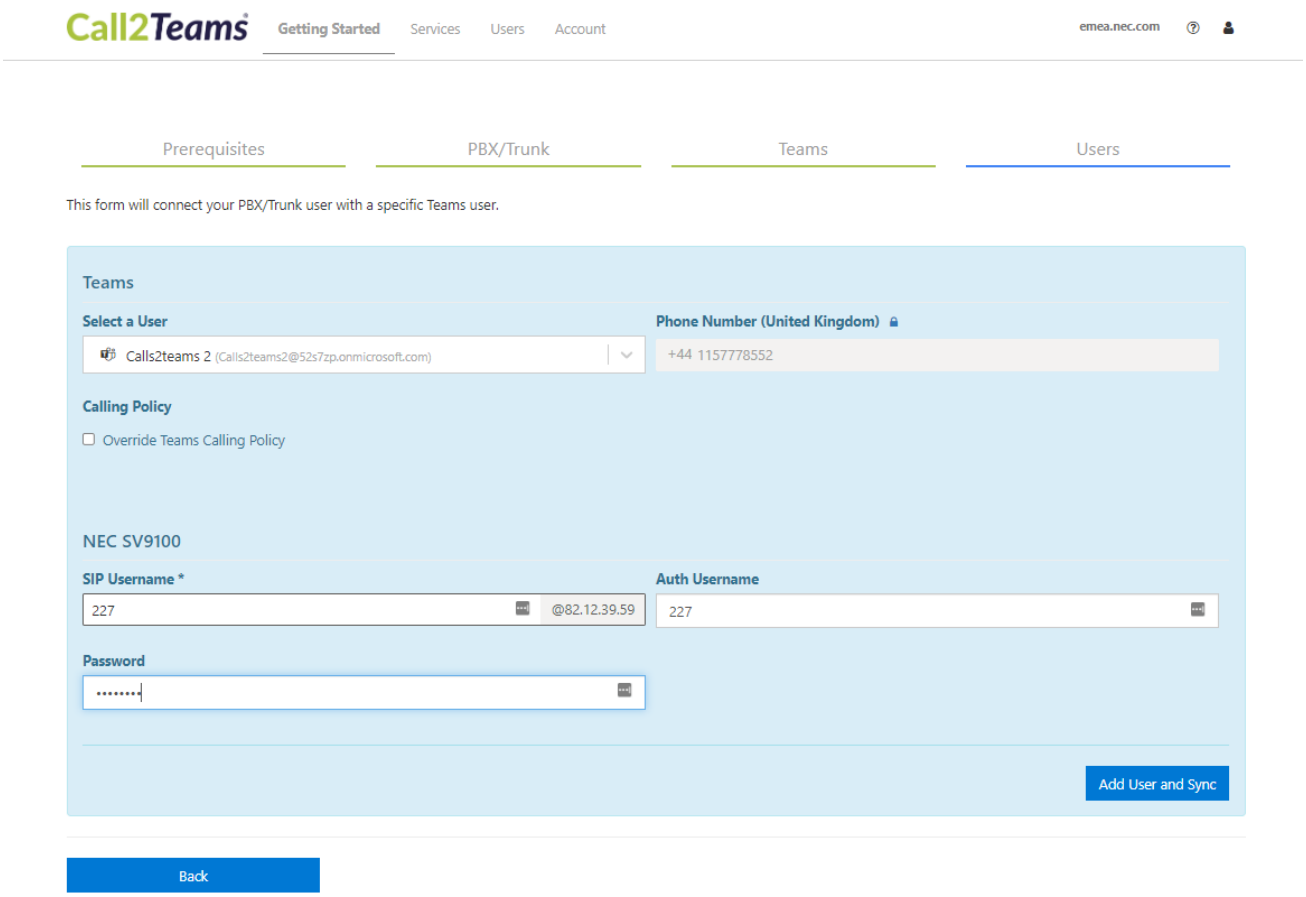


Setting Parameter	Value
Service Name	NEC SV9100
Country	As Applicable
SIP Domain	SV9100 Public IP address or FQDN
SIP Proxy	SV9100 Public IP address or FQDN, define port using :'portnumber'
Authentication Type	Registration
Calling Policy	Enable manage Teams Calling Policy
Teams Voicemail	Prohibit Voicemail
Music On Hold	PBX Hold Music
Protocol	Set As Applicable
Propagate Refer	PBX handles Transfer
Outside Line Prefix	Set As Applicable
E164 Number format	Localized
E164 Number Translation	Set As Applicable for the Region in question

3. Click Sync Now to sync the changes made to the Office 365 tenant. The action of clicking sync now will make the required changes to the office 365 Calling policy and import office 365 users who have the suitable licenses assigned. The sync can take up to 15 minutes to complete. Once the sync is completed click next.
   Meanwhile the sync takes place, a Call2Teams User can receive incoming calls, but cannot make Outbound calls (as there is no visible Keypad in the application). Once synced, the user needs to log out/ log back into MS Teams to see the Keypad.

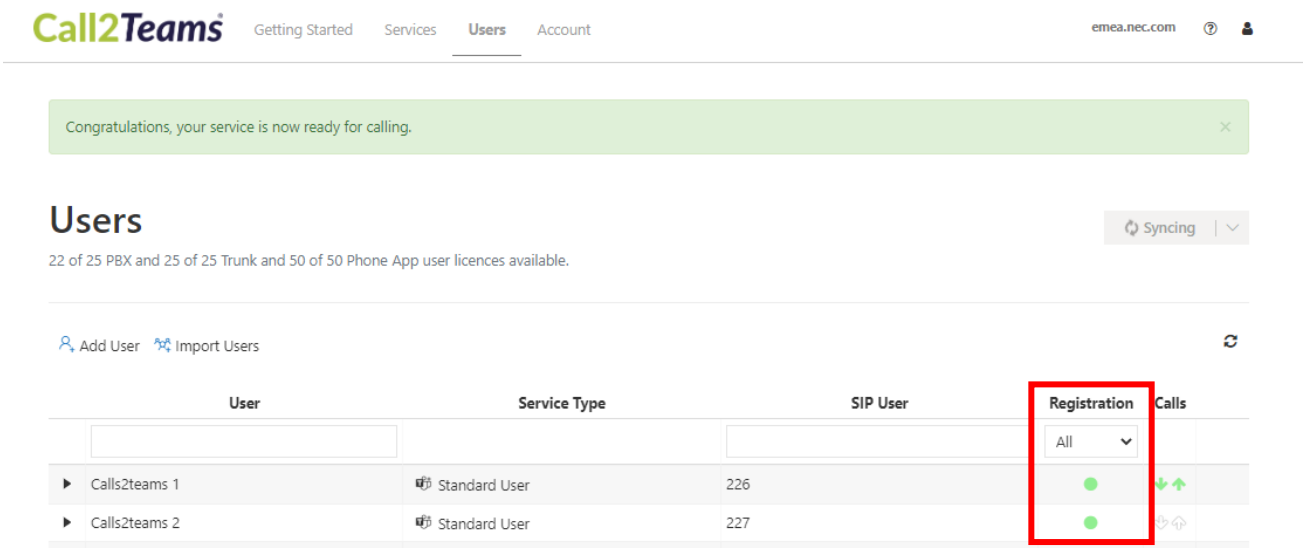


4. Complete the user template and click add User, followed by Sync. This stage creates a user which will register to the SV9100 3rd party SIP extension.

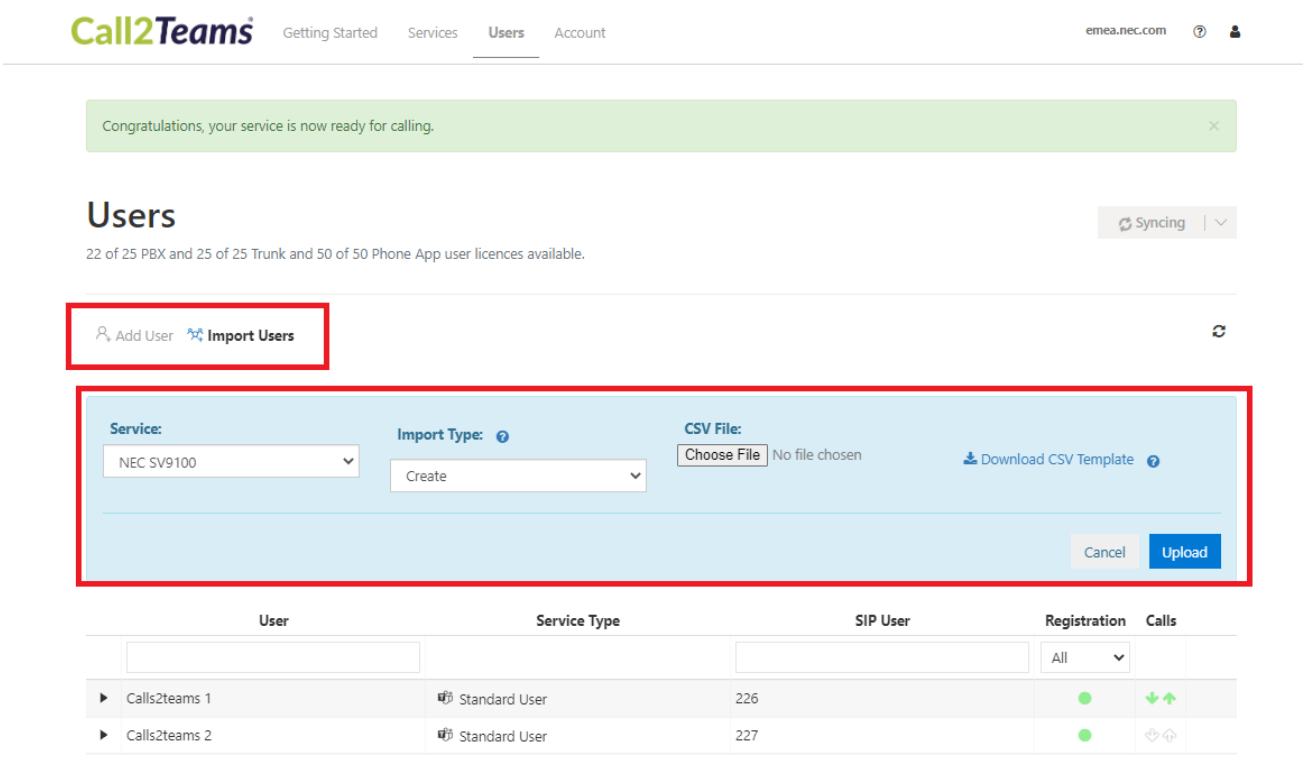


Setting Parameter	Value
Select User	Select the Office 365 user
Phone Number	Add a valid PSTN phone number
SIP Username	The SV9100 extension number
Auth Username	The SV9100 extension number
Password	The SIP password set on the SV9100 (15-05-16)

The registration status of a user can be reviewed in the Users tab. A green icon indicates a successful registration for the user.



5. To add further users click Add User or use the Import Users utility. Once all users are added click Sync now to sync the changes to the Office 365 tenant.

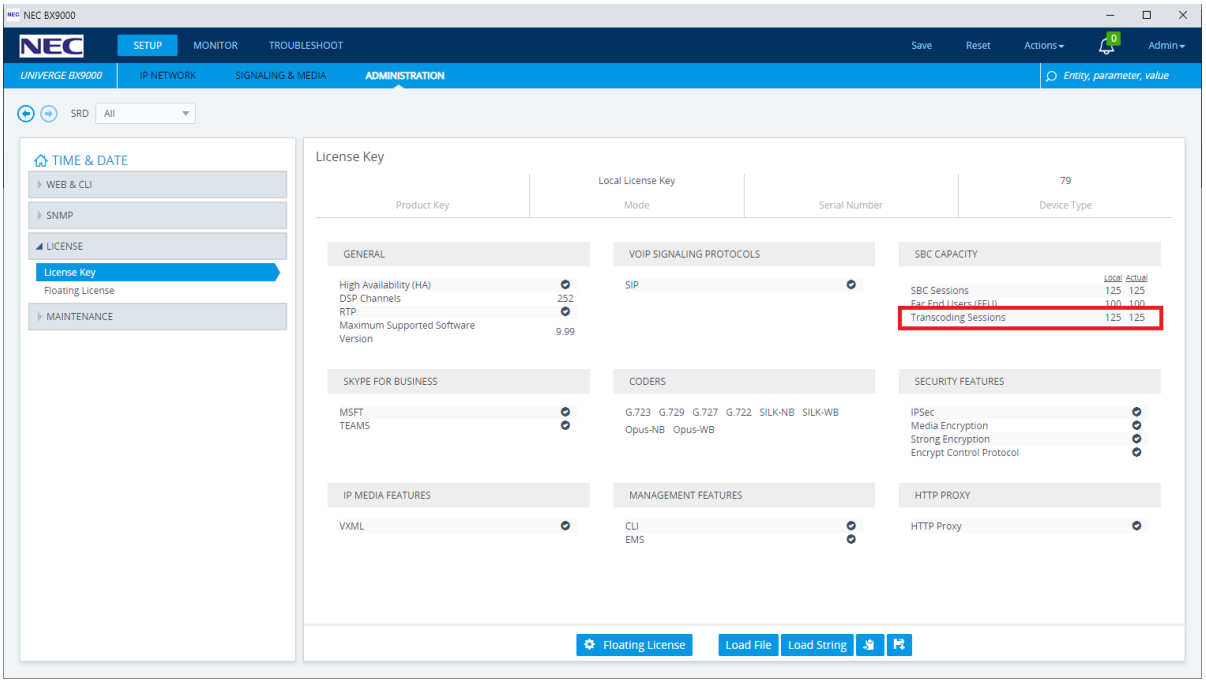


Configure Coder Transcoding (Optional)

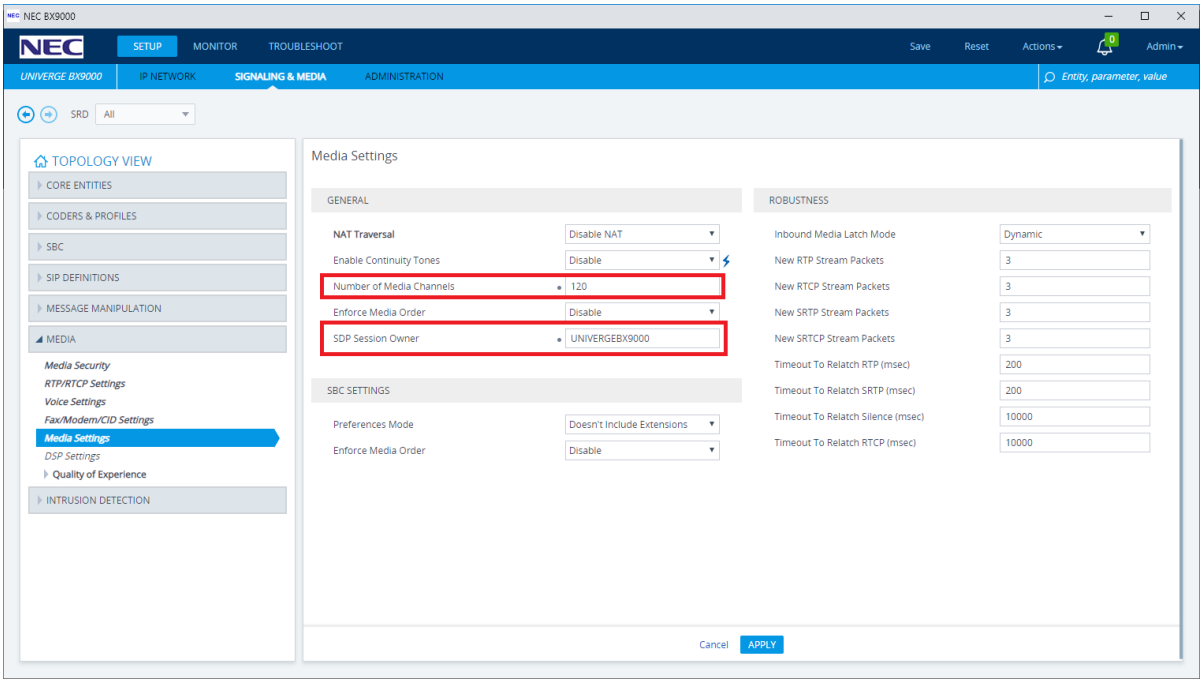
The SV9100 does not support SILK NB or SILK WB codecs. These codecs provide good properties for high latency connections, providing resiliency for lost or delayed RTP packets. The SBC is capable of transcoding calls. This feature requires hardware DSPs for the BX800 device, or virtual DSPs which are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

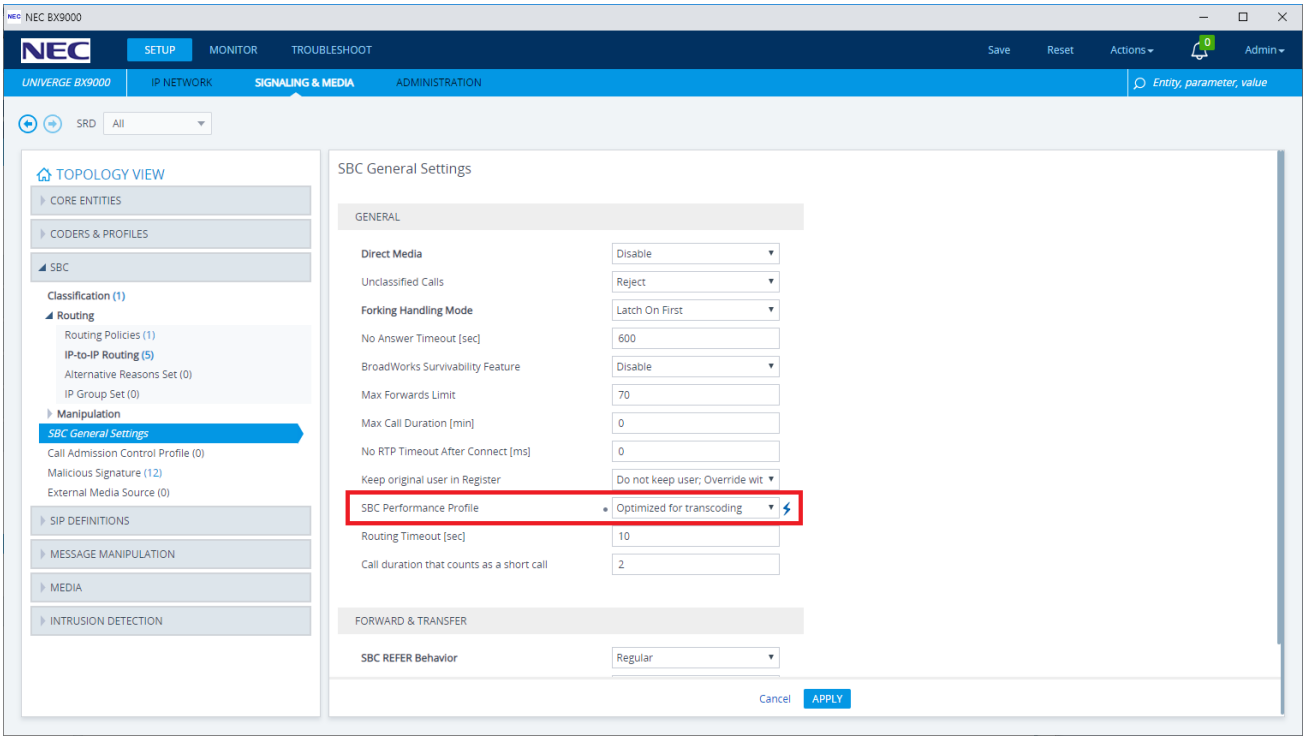
1. Ensure that you have a license key for Transcoding and the codecs are supported in *SETUP > ADMINISTRATION > LICENSE > License Key*.



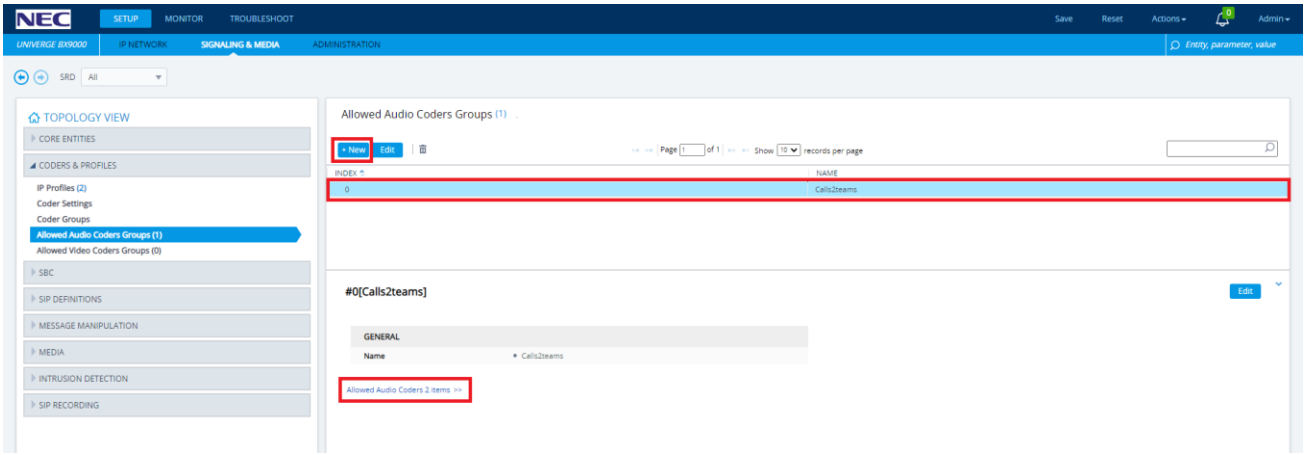
2. Enable the number of Media Channels in *SETUP > SIGNALING & MEDIA > MEDIA > Media Settings.* Also check that the SDP Session Owner does not contain any illegal characters (space).



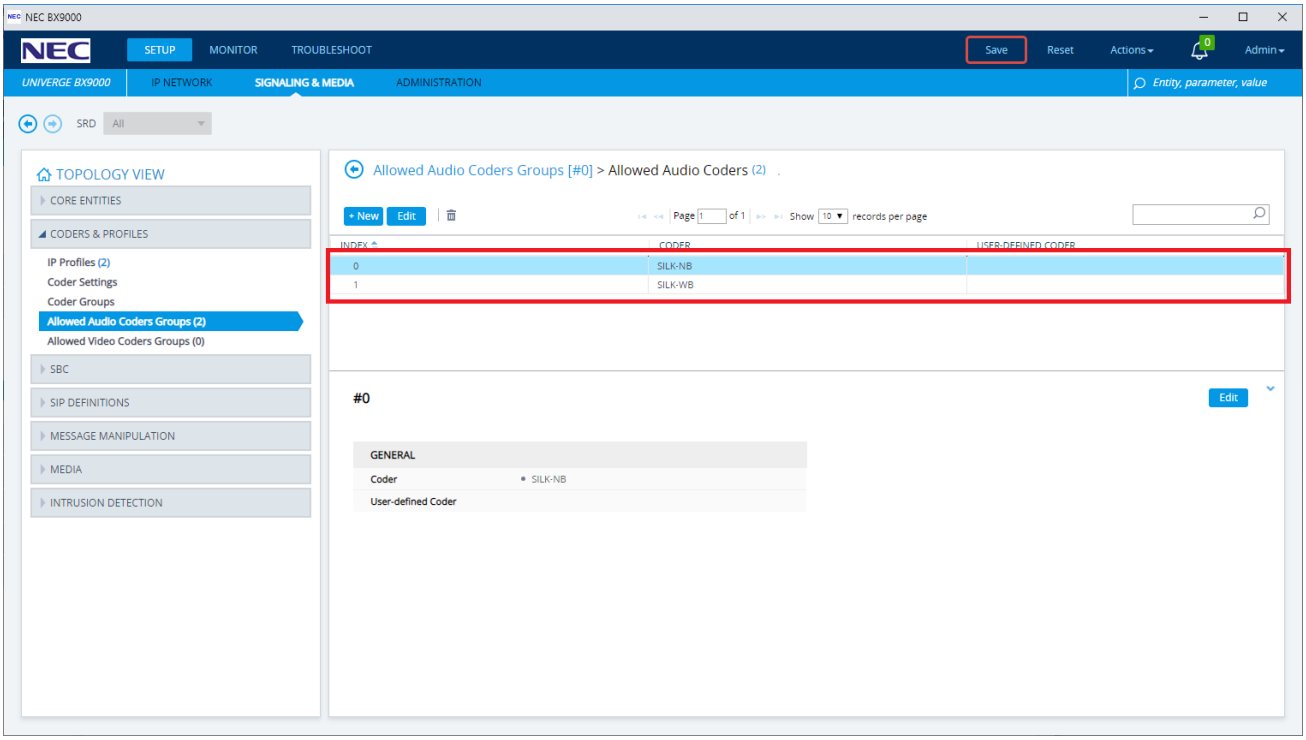
3. Enable Transcoding support in *SETUP > SIGNALING & MEDIA > SBC > SBC General Settings.*



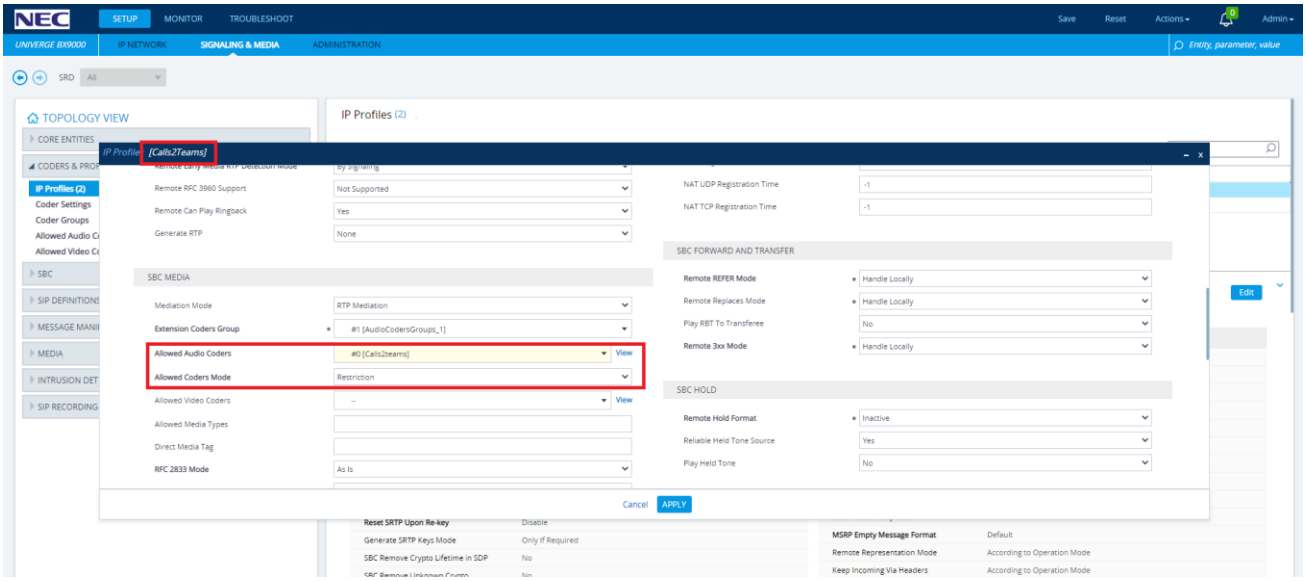
4. Create an 'Allowed' coder group for Calls2Teams in *SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Allowed Audio Coders Groups.* Open the child table.



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.

```
192.168.88.5 local0.notice [S=155625] [SID=21916f:114:5051] (N  142863) MRC::AllocateMediaResources [Time:15-02@23:06:26.118]
192.168.88.5 local0.notice [S=155626] [SID=21916f:114:5051] (N  142864) ConnectionData::CalculateResourcesForExtTranscoding Leading:DSP Opposite:CODERTRANSCODING MediationLevel:RTP [Time:15-02@23:06:26.119]
192.168.88.5 local0.notice [S=155627] [SID=21916f:114:5051] (N  142865) ResourceCounter: Coder Transcoding session +1 [1/125] [Time:15-02@23:06:26.119]
192.168.88.5 local0.notice [S=155628] [SID=21916f:114:5051] (N  142866) ResourceCounter: Media channel +1 [1/120] [Time:15-02@23:06:26.119]
192.168.88.5 local0.notice [S=155629] [SID=21916f:114:5051] (N  142867) <(#253)>CID=-100 ChannelResource::AllocateResource DSP Allocated. Available count 1021 [Time:15-02@23:06:26.119]
192.168.88.5 local0.notice [S=155630] [SID=21916f:114:5051] (N  142868) ResourceCounter: Media channel +1 [2/120] [Time:15-02@23:06:26.119]
192.168.88.5 local0.notice [S=155631] [SID=21916f:114:5051] (N  142869) <(#254)>CID=-100 ChannelResource::AllocateResource DSP Allocated. Available count 1020 [Time:15-02@23:06:26.119]
192.168.88.5 local0.notice [S=155632] [SID=21916f:114:5051] (N  142870) (#279)RTS::AllocateResource CODERTRANSCODING already Allocated. [Time:15-02@23:06:26.119]
192.168.88.5 local0.notice [S=155633] [SID=21916f:114:5051] (N  142871) (#278)RTS::AllocateResource DSP already Allocated. [Time:15-02@23:06:26.119]
```

TLS Configuration (Optional)

It is possible to register Qunifi Ltd.'s Call2Teams for Microsoft® Teams service to the NEC BX gateway using TLS. In this section steps will be detailed to register to the BX gateway using TLS, the internal leg between the BX SBC and the NEC platform will remain unencrypted.

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 included in the Mozilla Foundation trusted CA list (https://wiki.mozilla.org/CA).

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.

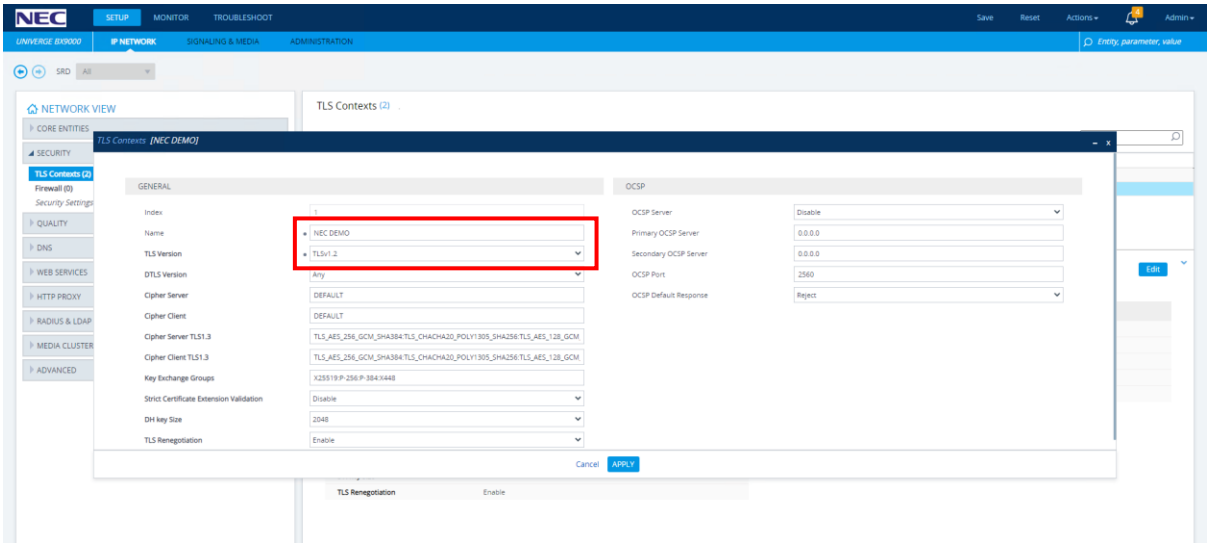
Configure your TLS Context

To load your TLS Security Certificate into the BX;

1. Log into the web interface of the BX
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.

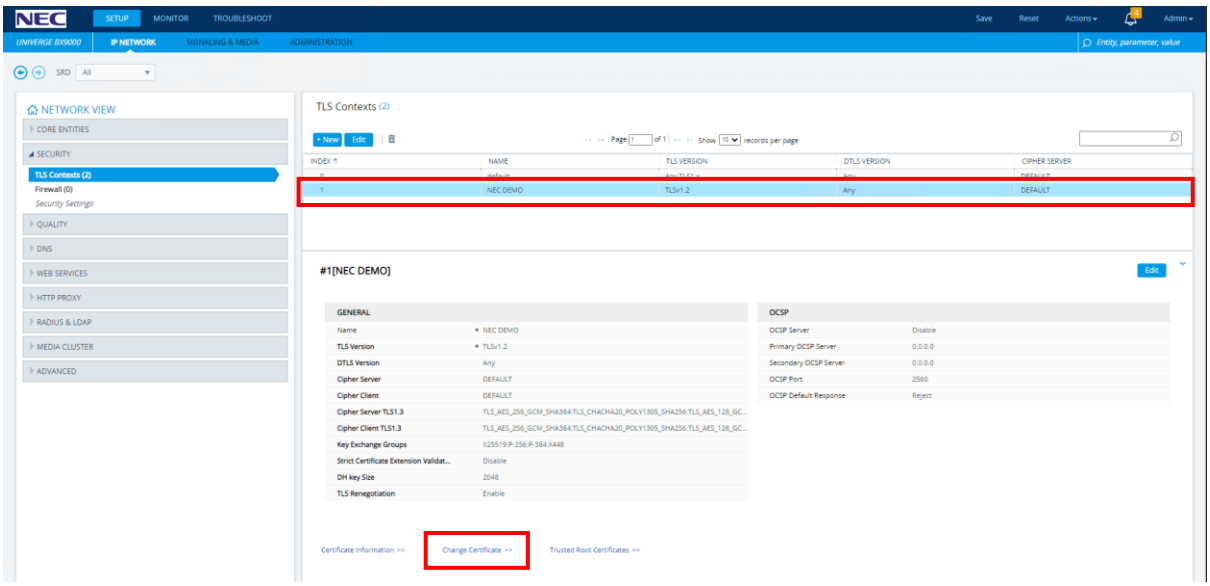
In the screenshot below a new TLS context has been created called 'NECDEMO', replace this name with your customer name and ensure that only TLSv1.2 is enabled.



Deploy the Certificates and Private Key

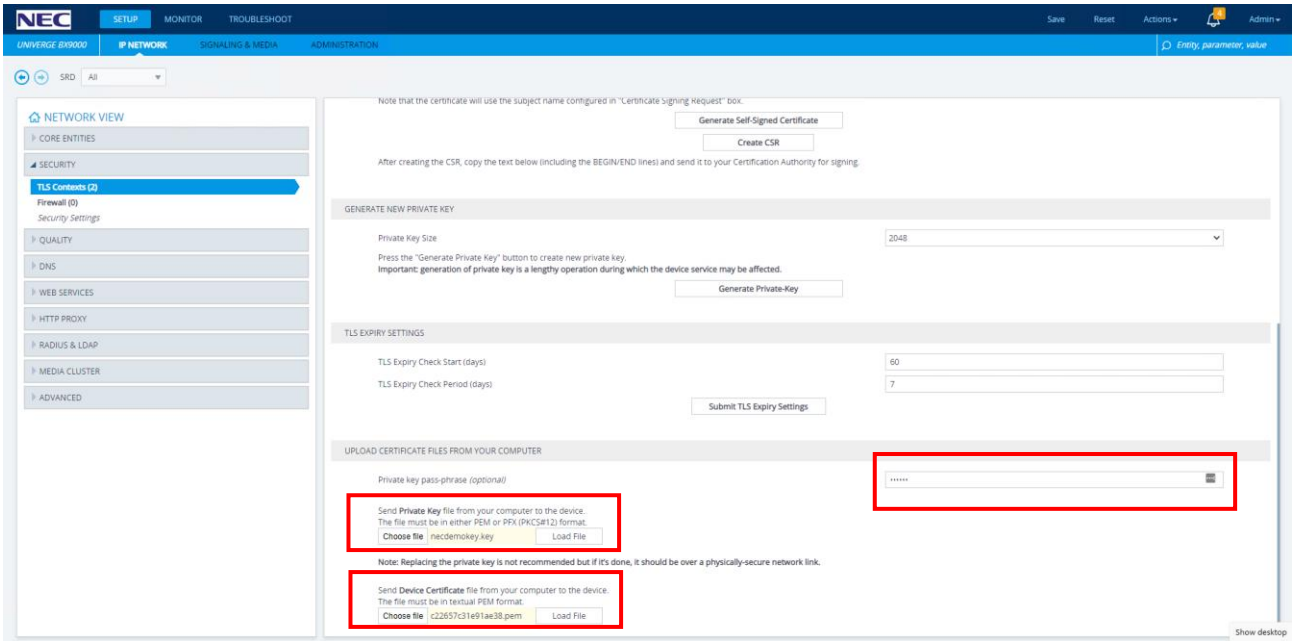
In the SBC Web GUI return to the TLS Contexts page and complete the following;

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

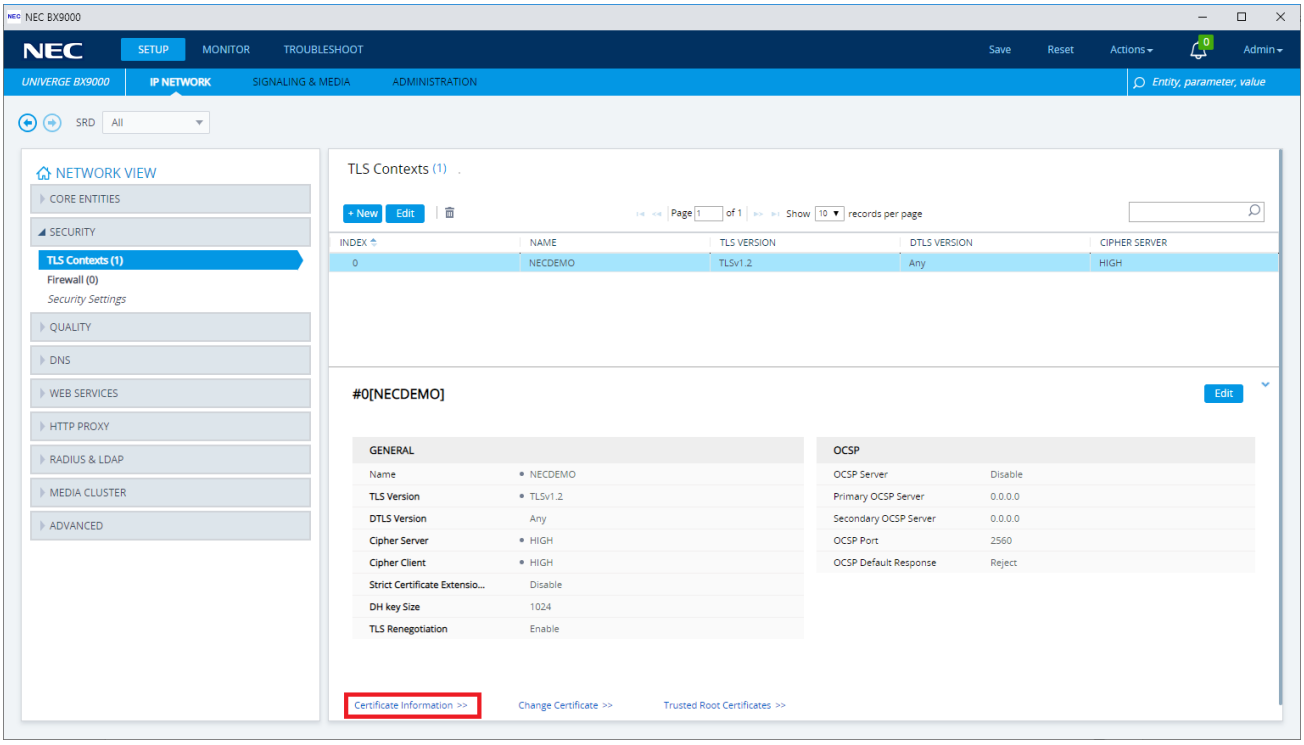


2. Scroll down to the *UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER* group and upload your Private Key file and Device Certificate files*. If the Private Keu file is encrypted then enter the password in the pass-phrase box. When you upload the files you will see a verification if successful.

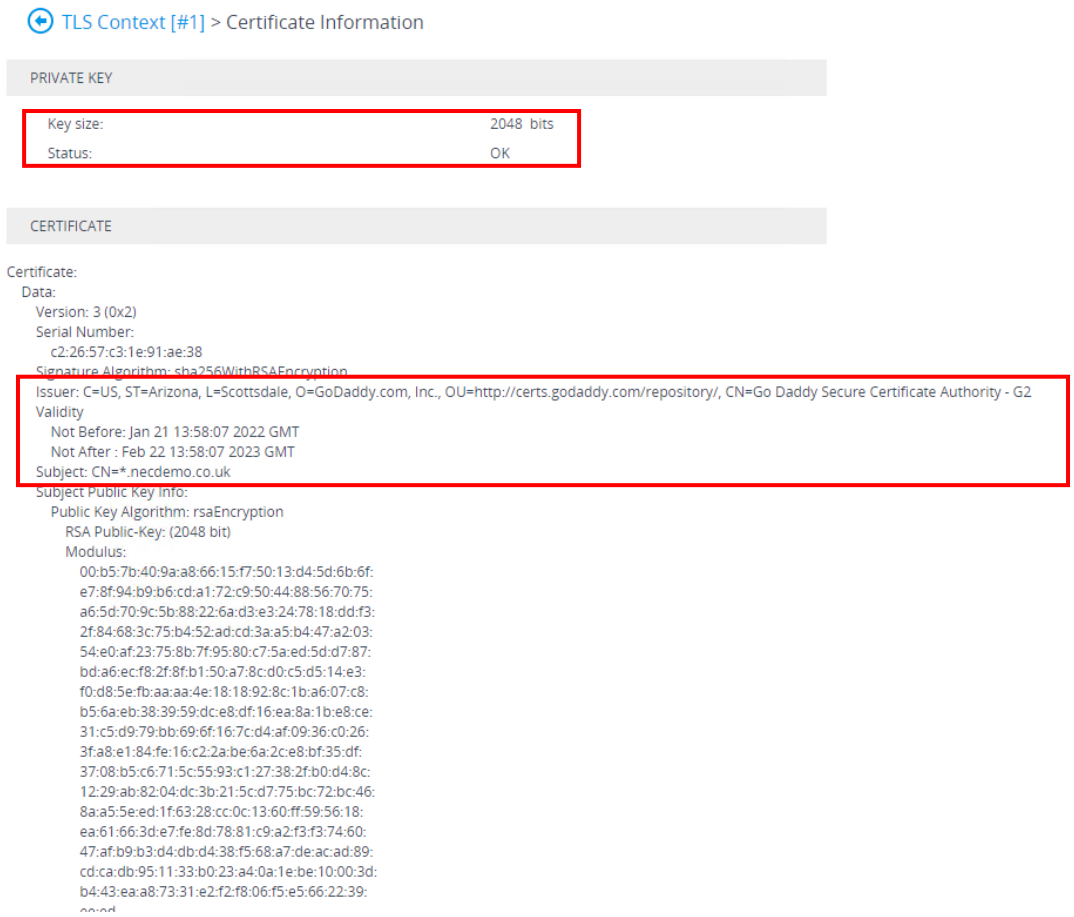
* The uploaded certificate files should be PEM encoded with .pem, .cer or .crt file extension.



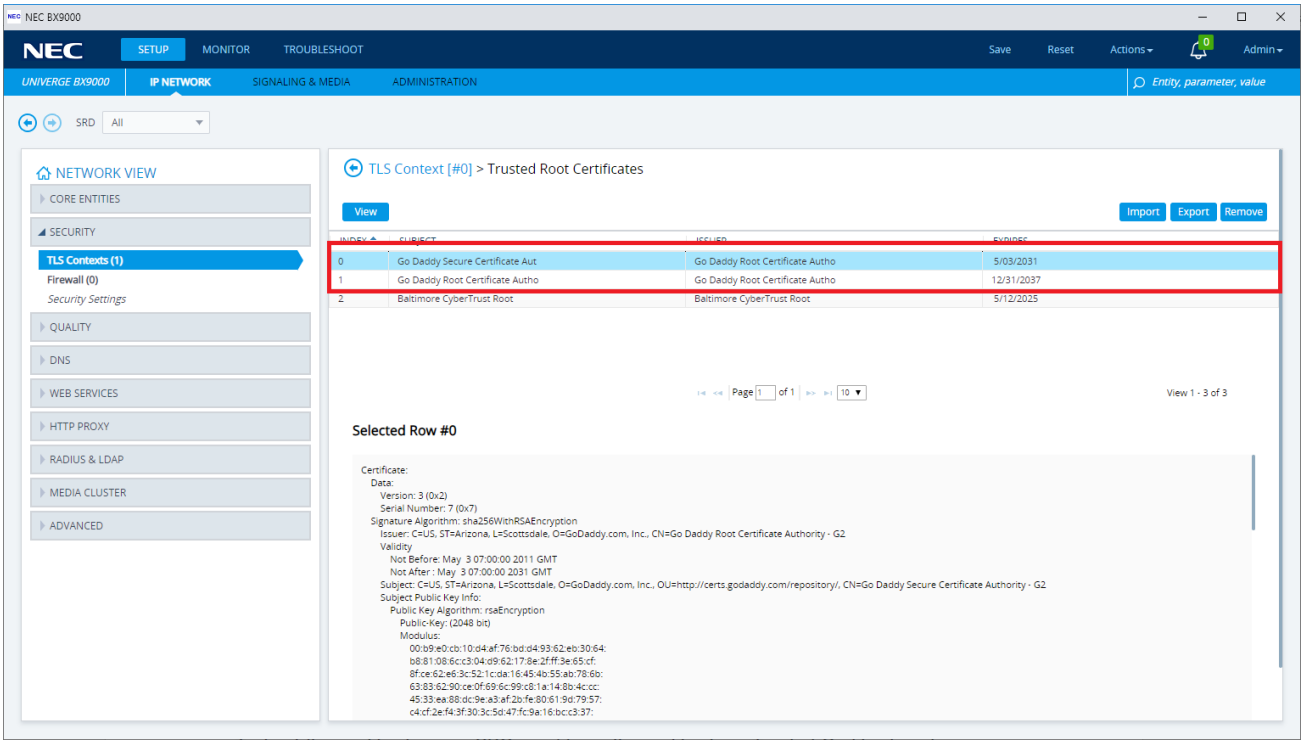
3. Validate that the certificate and private key were uploaded correctly. From the TLS Contexts page, choose the *Certificate Information* link to see detail about the uploaded certificate.



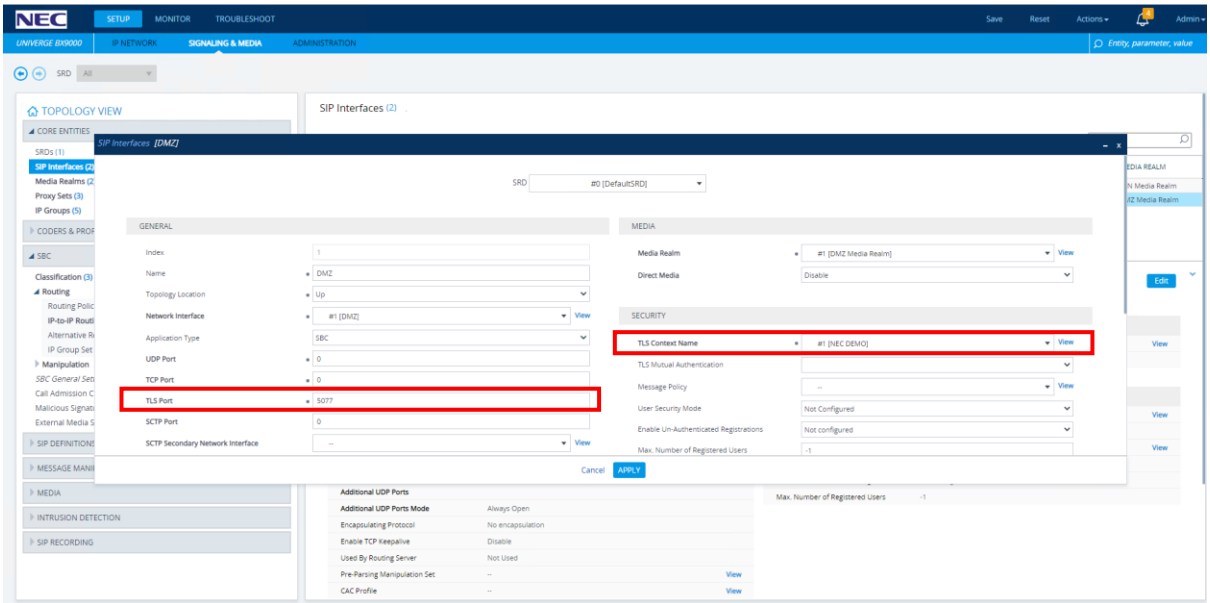
4. If the Status is OK then you can continue to the next steps, otherwise go back and check the uploaded files.



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.

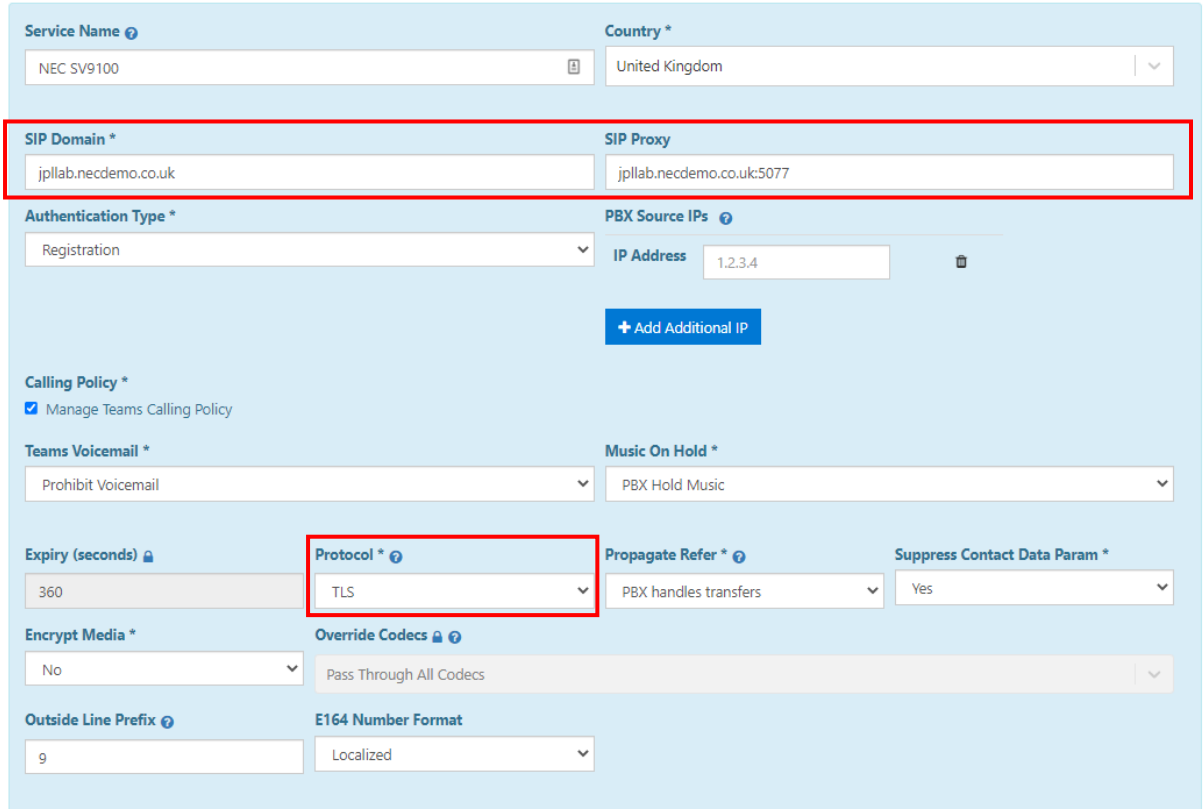


6. Navigate to *SETUP > SIGNALING & MEDIA > SIP Interfaces.* Select the DMZ SIP interface, configure a suitable port number as the TLS port and assign the previously created TLS context name to the interface.



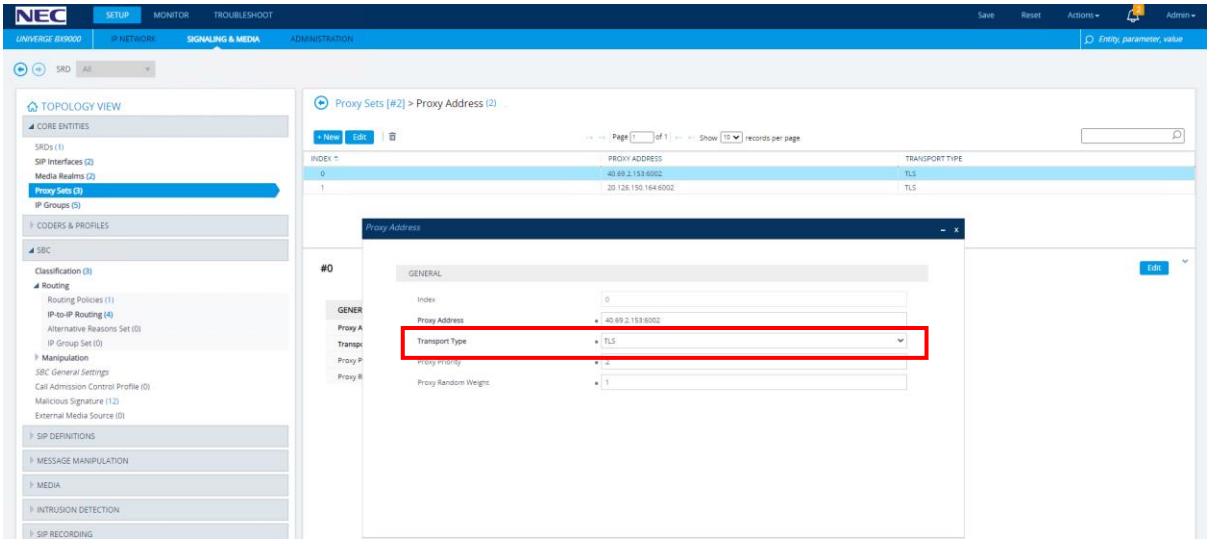
Calls2Teams TLS configuration

Change the SIP Domain and SIP proxy as required. In this example we use JPLLAB.NECDEMO.CO.UK as the server certificate is a wild card for the domain NECDEMO.CO.UK. The SIP domain and SIP proxy must be included in the CN and SAN's of your server certificate. Change the protocol to TLS, save the changes, and sync the changes.



Note during testing it was noticed that changing the protocol to TLS can result in the SBCs used by Calls2Teams changing. The SBCs should be verified and if changed these changes should be reflected on the BX SBC proxy sets and customer's firewall.

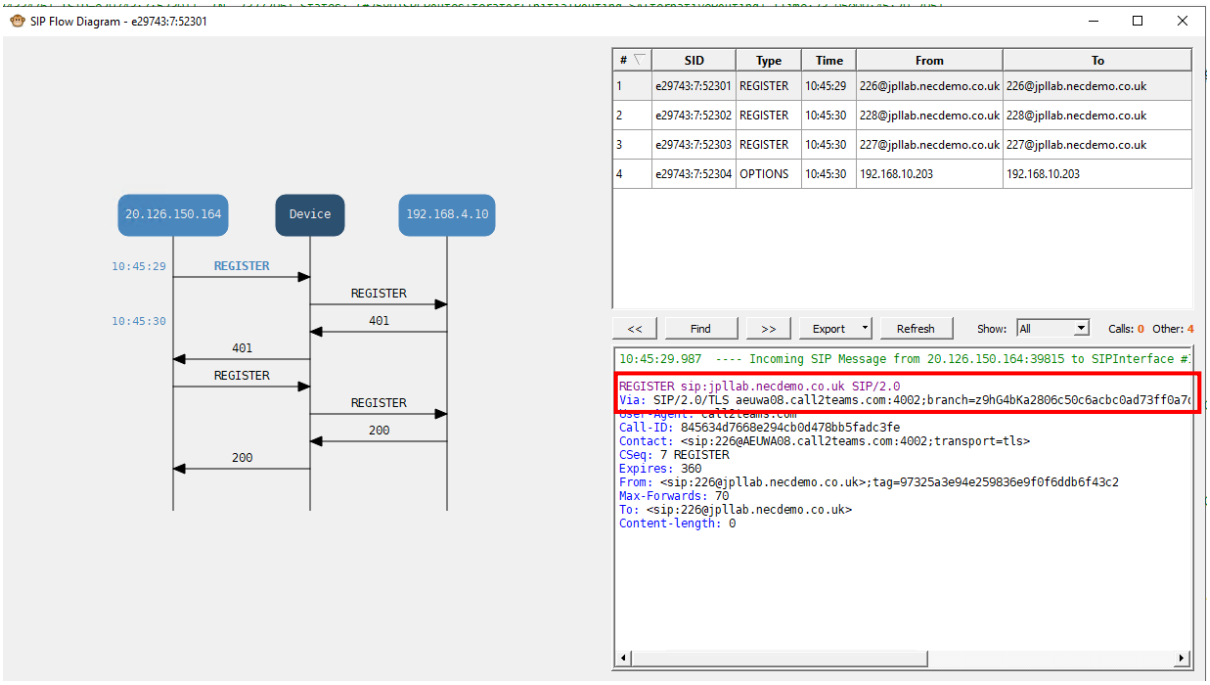
The change of protocol needs to be reflected in the SBC. Navigate to *SETUP > SIGNALING & MEDIA > CORE ENTITIES > Proxy Sets* and change the transport type for both indexes on the Calls2Teams proxy set to TLS.



To confirm registration has taken place via TLS the registration status can be checked on the user tab.

User	Service Type	SIP User	Registration	Calls
			All	
Calls2teams 1	Standard User	226		
Kit 2	Standard User	228		
Calls2teams 2	Standard User	227		

The SBC syslog can also be checked to confirm registration via TLS has taken place.



Tested Call Scenarios

Below is a list of tested call scenarios with SV9100 and Calls2Teams.

Call scenarios that are not detailed in the below table have not been tested. NEC therefore cannot guarantee the operation of any call scenarios not detailed in the below table.

Index	Category	Description	Pass / Fail	Remarks
0	Basic call operation	Internal call between NEC TDM terminal and Calls2Teams	Pass	
1	Basic call operation	Internal call between NEC IP terminal and Calls2Teams	Pass	
2	Basic call operation	Internal call between two Calls2Teams users	Pass	
3	Basic call operations	Internal call between a 3rd party SIP extension and Calls2Teams	Pass	
4	Basic call operation	DDI routing (22-11) direct to Calls2Teams extension in target 1	Pass	
5	Basic call operation	Membership of SV9100 Incoming ring group	Pass	Teams voicemail must be disabled - The teams user will display a missed call if the call is answered by another user
6	Basic call operation	Membership of SV9100 Department group	Pass	Teams voicemail must be disabled - The teams user will display a missed call if the call is answered by another user
7	Call transfer	Blind transfer from an SV9100 extension to a Calls2Teams extension	Pass	SV party shows as CLI on Teams client
8	Call transfer	Supervised transfer from an SV9100 extension to a Calls2Teams extension	Pass	SV party shows as CLI on Teams client
9	Call transfer	Blind transfer of an external call from a Calls2Teams extension to an SV9100 extension	Pass	Note - Teams users have to hang-up the call as Teams unaware that the PSTN call is connected with the SV extension
10	Call transfer	Supervised transfer of an external call from a Calls2Teams extension to an SV9100 extension	Pass	
11	Call transfer	Supervised transfer of an internal call from a Calls2Teams extension to an SV9100 extension	Pass	
12	Call transfer	Blind transfer of an internal call from a Calls2Teams extension to an SV9100 extension	Pass	
13	Call transfer	Supervised transfer of an internal call from a Calls2Teams extension to an SV9100 extension	Pass	
14	Call transfer	Blind transfer of an internal call from a SV9100 extension to an Calls2Teams extension	Pass	
15	Call transfer	Supervised transfer of an internal call from a SV9100 extension to an Calls2Teams extension	Pass	
15	Call transfer	Blind transfer of an external from a Calls2Teams extension to a trunk	Pass	Note - Teams users have to hang-up the call as Teams unaware that the PSTN call is connected with the SV extension
16	Call transfer	Supervised transfer of an external call from a Calls2Teams extension to a trunk	Pass	
17	Call transfer	Blind transfer of an external call from a Calls2Teams extension to another Calls2Teams extension		Note - Teams users have to hang-up the call as Teams unaware that the PSTN call is connected with the SV extension. The transfer was tested using the

				SV9100 extension numbers. Call transfer within the Teams environment is not supported.
18	Call transfer	Supervised transfer of an external from a Calls2Teams extension to another Calls2Teams extension	Pass	
19	Call hold	Place and recall calls from hold	Pass	PBX music on hold is played to the held party

Limitations

SV9100 feature codes beginning with '*' that can be dialed. Most will work from Teams, but *11, *12 and *13 do not. Microsoft has indicated that they reserve the right to block some other two-digit star codes as they allocate them for new native Teams features. If you use these blocked feature codes, you will need to change them to codes that Teams will not block.

Numbers beginning with '0' are converted to E164 format. If you have extension numbers beginning with '0', consider changing them so they do not have this prefix