

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

Version History	1
Purpose of this document:	3
Scope of this document.....	3
Calls2Teams description	3
Prerequisites.....	3
Test Network	5
General BX SBC Configuration	6
Configure IP Interfaces and NAT Traversal.....	6
Configure Media Realms	7
Configure SIP Interfaces	8
Configure Proxy Sets and Proxy Addresses	8
Configure Coder Groups.....	11
Configure the IP Profile for Calls2Teams	12
Configure the IP Profile for the SV9100	13
Configure IP Groups.....	14
Configure Classification conditions	16
Configure IP-to-IP Routing Rules	18
Configure INI Parameters	19
SV9100 Configuration	20
IP Extension Setup	20
Calls2Teams Configuration	22
Calls2Teams Configuration Wizard.....	22
Configure Coder Transcoding (Optional)	27
TLS Configuration (Optional)	31
Configure your TLS Context.....	31
Deploy the Certificates and Private Key	31
Calls2Teams TLS configuration	35

Tested Call Scenarios.....37

Limitations38

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

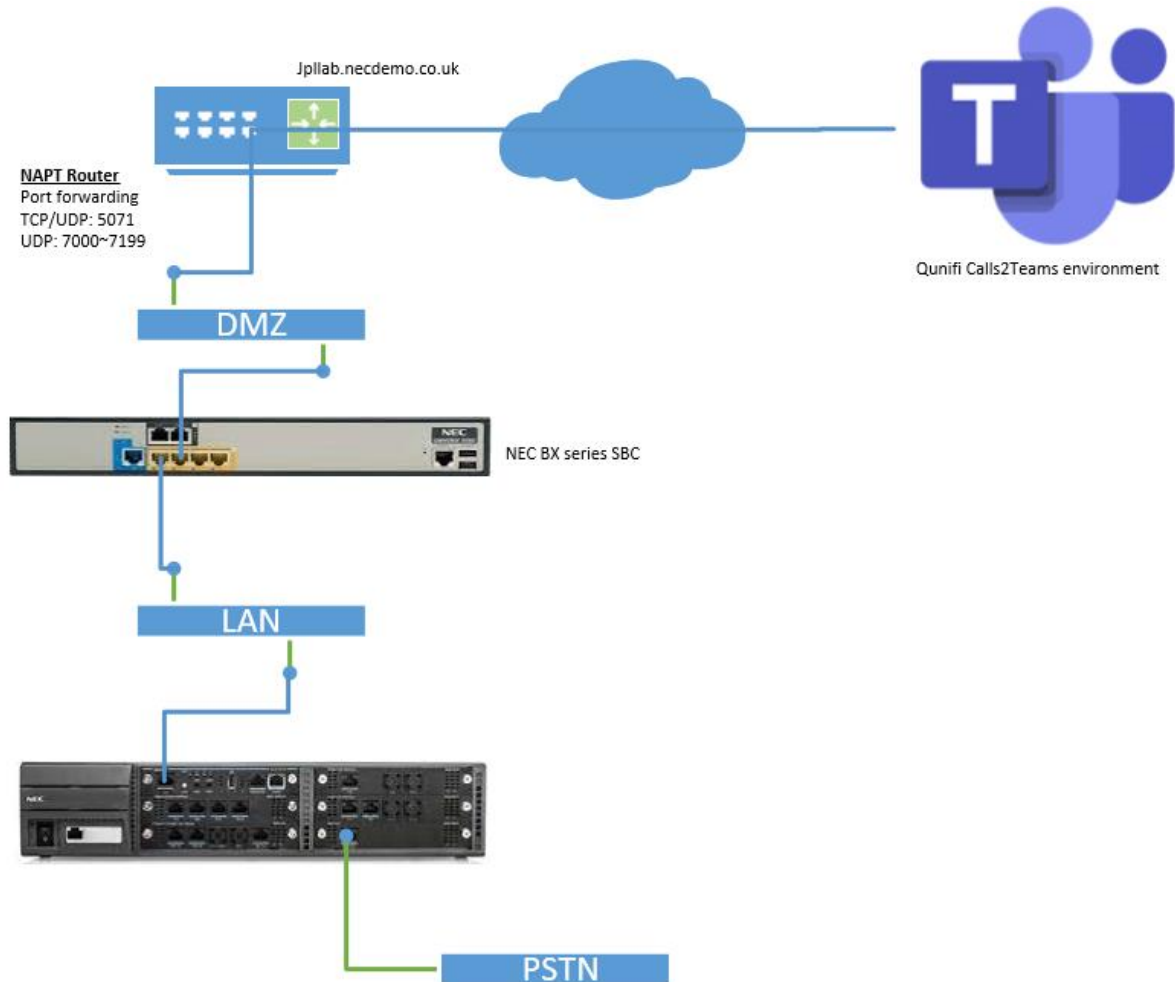
Network Infrastructure

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.

The screenshot displays the NEC SBC configuration interface. On the left, the 'NETWORK VIEW' sidebar shows a tree of configuration categories: CORE ENTITIES, IP Interfaces (2), Ethernet Devices (2), Ethernet Groups (15), Physical Ports (2), Static Routes (0), HA Settings, HA Network Monitor (0), NAT Translation (2), SECURITY, QUALITY, DNS, WEB SERVICES, HTTP PROXY, RADIUS & LDAP, MEDIA CLUSTER, and ADVANCED. The 'NAT Translation (2)' item is selected and highlighted in blue. The main panel shows the 'NAT Translation (2)' configuration page. It includes a table with 7 columns: INDEX, SOURCE INTERFACE, TARGET IP ADDRESS, SOURCE START PORT, SOURCE END PORT, TARGET START PORT, and TARGET END PORT. Two rows are listed, both with a SOURCE INTERFACE of 'DMZ'. The first row (INDEX 0) has a TARGET IP ADDRESS of '82.12.39.59', SOURCE START PORT of '5070', SOURCE END PORT of '5071', TARGET START PORT of '5070', and TARGET END PORT of '5071'. The second row (INDEX 1) has a TARGET IP ADDRESS of '82.12.39.59', SOURCE START PORT of '7000', SOURCE END PORT of '7199', TARGET START PORT of '7000', and TARGET END PORT of '7199'. Below the table, there is a detailed view for the selected entry (INDEX 0), showing 'SOURCE' and 'TARGET' parameters. The SOURCE parameters are: Source Interface (DMZ), Source Start Port (5070), and Source End Port (5071). The TARGET parameters are: Target IP Address (82.12.39.59), Target Start Port (5070), and Target End Port (5071).

INDEX	SOURCE INTERFACE	TARGET IP ADDRESS	SOURCE START PORT	SOURCE END PORT	TARGET START PORT	TARGET END PORT
0	DMZ	82.12.39.59	5070	5071	5070	5071
1	DMZ	82.12.39.59	7000	7199	7000	7199

#0

SOURCE		TARGET	
Source Interface	DMZ	Target IP Address	82.12.39.59
Source Start Port	5070	Target Start Port	5070
Source End Port	5071	Target End Port	5071

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

The screenshot shows the NEC UNIVERGE B10000 web interface. The left sidebar contains a 'TOPOLOGY VIEW' section with 'CORE ENTITIES' expanded, showing 'SIP Interfaces (2)', 'Media Realms (2)', 'Proxy Sets (3)', and 'IP Groups (4)'. The 'Media Realms (2)' item is selected. The main area displays a table of Media Realms:

INDEX	NAME	IPv4 INTERFACE NAME	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM
0	LAN Media Realm	LAN	6000	50	6199	Yes
1	DMZ Media Realm	DMZ	7000	50	7199	No

Below the table, the configuration details for the LAN Media Realm are shown:

#0[LAN Media Realm]

GENERAL

- Name: LAN Media Realm
- Topology Location: Down
- IPv4 Interface Name: LAN
- UDP Port Range Start: 6000
- Number Of Media Session Legs: 50
- UDP Port Range End: 6199
- TCP Port Range Start: 0
- TCP Port Range End: 0
- Default Media Realm: Yes
- Used By Routing Server: Not Used

QUALITY OF EXPERIENCE

- QoS Profile: --
- Bandwidth Profile: --

The screenshot shows the NEC UNIVERGE B10000 web interface. The left sidebar contains a 'TOPOLOGY VIEW' section with 'CORE ENTITIES' expanded, showing 'SIP Interfaces (2)', 'Media Realms (2)', 'Proxy Sets (3)', and 'IP Groups (4)'. The 'Media Realms (2)' item is selected. The main area displays a table of Media Realms:

INDEX	NAME	IPv4 INTERFACE NAME	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM
0	LAN Media Realm	LAN	6000	50	6199	Yes
1	DMZ Media Realm	DMZ	7000	50	7199	No

Below the table, the configuration details for the DMZ Media Realm are shown:

#1[DMZ Media Realm]

GENERAL

- Name: DMZ Media Realm
- Topology Location: Up
- IPv4 Interface Name: DMZ
- UDP Port Range Start: 7000
- Number Of Media Session Legs: 50
- UDP Port Range End: 7199
- TCP Port Range Start: 0
- TCP Port Range End: 0
- Default Media Realm: No
- Used By Routing Server: Not Used

QUALITY OF EXPERIENCE

- QoS Profile: --
- Bandwidth Profile: --

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.

The screenshot displays the NEC SIP Interfaces configuration page. On the left, a sidebar shows the navigation menu with options like TOPOLOGY VIEW, CORE ENTITIES, SRDs, SIP Interfaces (2), Media Realms (2), Proxy Sets (3), IP Groups (4), CODERS & PROFILES, SBC, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, INTRUSION DETECTION, and SIP RECORDING. The main area shows a table of SIP Interfaces. The table has columns: INDEX, NAME, SRD, NETWORK INTERFACE, APPLICATION TYPE, UDP PORT, TCP PORT, TLS PORT, ENCAPSULATING PROTOCOL, and MEDIA REALM. Two interfaces are listed: 0 (LAN) and 1 (DMZ). Below the table, the configuration details for the selected interface (LAN) are shown, including General, Media, and Security settings.

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	LAN	DefaultSRD (SR)	LAN	SBC	5070	5070	0	No encapsulation	LAN Media Realm
1	DMZ	DefaultSRD (SR)	DMZ	SBC	5071	5071	5061	No encapsulation	DMZ Media Realm

Below the table, the configuration details for the selected interface (LAN) are shown, including General, Media, and Security settings.

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.

INDEX	PROXY ADDRESS	TRANSPORT TYPE
0	192.168.4.10:5070	UDP

- 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.

The screenshot shows the NEC UNIVERGE BX9000 administration interface. The left sidebar contains a 'TOPOLOGY VIEW' menu with options like SRDs, SIP Interfaces, Media Realms, Proxy Sets, and IP Groups. The main area displays the 'Proxy Sets (3)' configuration. A table lists three proxy sets, with the second one, 'Calls2Teams', highlighted in red. Below this, the configuration details for '#2[Calls2Teams]' are shown, including 'SBC IP4 SIP Interface' set to 'DNZ', 'Proxy Keep-Alive' set to 'Using OPTIONS', and 'Proxy Load Balancing Method' set to 'Random Weights'. The 'Proxy Address' table at the bottom shows two entries: '40.69.2.153:6002' and '20.126.150.164:6002', both using 'UDP' transport type.

Proxy Sets [#2] > Proxy Address (2)

INDEX	PROXY ADDRESS	TRANSPORT TYPE
0	40.69.2.153:6002	UDP
1	20.126.150.164:6002	UDP

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.

The screenshot displays the NEC UniVerse 8X9000 interface for configuring Coder Groups. The main configuration area shows a table of codecs with the following data:

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
SILK-NB	20	8	104	N/A	
SILK-WB	20	16	103	N/A	
G.711A-law	20	64	8	Disabled	
G.729	20	8	18	Disabled	
G.722	20	64	9	Disabled	

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.

The screenshot shows the NEC management interface for configuring an IP Profile named 'Calls2Teams'. The interface is divided into several sections:

- GENERAL:**
 - Index: 1
 - Name: Calls2Teams
 - Created by: Routing Server
- MEDIA SECURITY:**
 - SBC Media Security Mode: As Is
 - Symmetric MKI: Disable
 - MKI Size: 0
 - SBC Enforce MKI Size: Don't enforce
 - SBC Media Security Method: SDES
 - Reset SRTP Upon Re-key: Disable
 - Generate SRTP Keys Mode: Only if Required
- SBC SIGNALING:**
 - PRACK Mode: Transparent
 - P-Asserted-Identity Header Mode: As Is
 - Diversion Header Mode: As Is
 - History-Info Header Mode: As Is
 - Session Expires Mode: Transparent
 - SIP UPDATE Support: Supported
 - Remote re-INVITE: Supported
 - Remote Delayed Offer Support: Supported
 - MSRP re-INVITE/UPDATE: Supported
 - MSRP Offer Setup Role: AcqPass
 - MSRP Empty Message Format: Default
 - Remote Representation Mode: According to Operation Mode
- SBC EARLY MEDIA:**
 - Remote Early Media: Supported
 - Remote Multiple 18x: Supported
 - Remote Early Media Response Ty...: Transparent
 - Remote Multiple Early Dialogs: According to Operation Mode
 - Remote Multiple Answers Mode: Disable
- Other Parameters:**
 - Keep User-Agent Header: According to Operation Mode
 - Handle X-Detect: No
 - ISUP Body Handling: Transparent
 - ISUP Variant: Itu92
 - Max Call Duration [min]: 0

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.

The screenshot shows the NEC Univerge BX9000 configuration interface. The 'IP Groups (4)' window is open, displaying the configuration for the 'Calls2Teams IP Group'. The 'GENERAL' tab is selected, showing fields for Name, Topology Location, Type, Proxy Set, IP Profile, Media Realm, Internal Media Realm, Contact User, and SIP Group Name. The 'QUALITY OF EXPERIENCE' tab shows QoS Profile and Bandwidth Profile. The 'MESSAGE MANIPULATION' tab shows Inbound and Outbound Message Manipulation Sets. The 'SBC GENERAL' tab shows SBC Group Name, Created By Routing Server, Used By Routing Server, Proxy Set Connectivity, and Classify By Proxy Set. The 'SBC REGISTRATION AND AUTHENTICATION' tab shows Max. Number of Registered Users, Registration Mode, and User Stickiness.

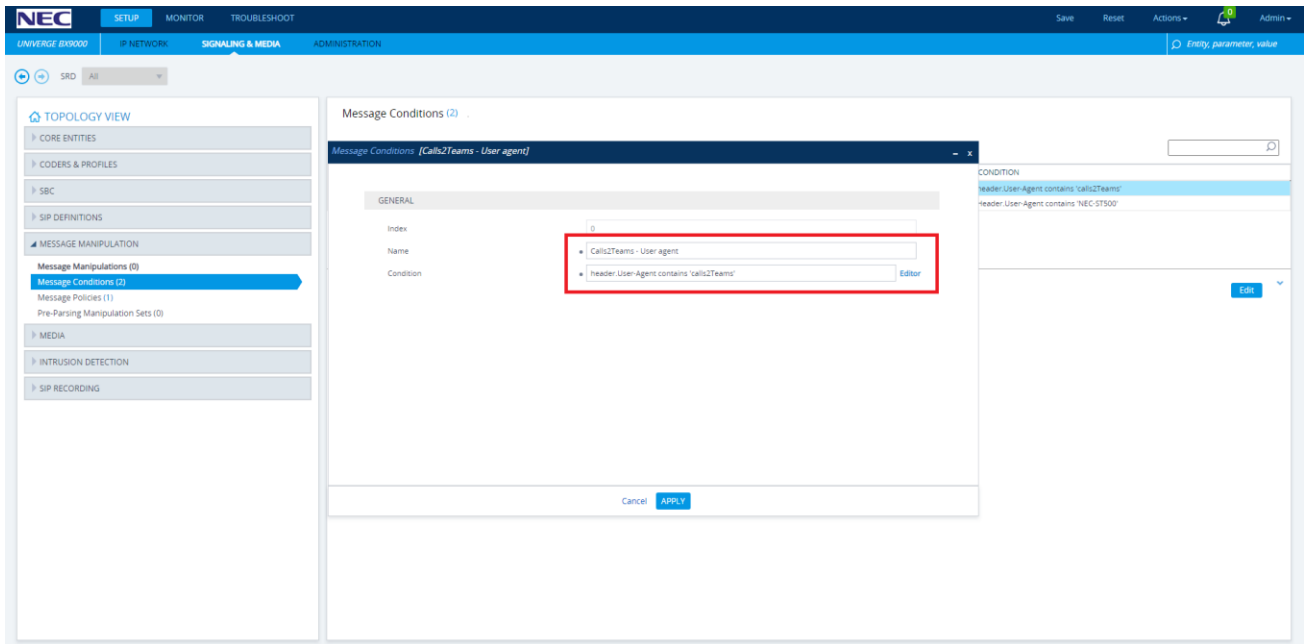
Name	Parameter
General	
Name	MS Teams (arbitrary descriptive name)
Topology Location	Up
Type	Server
Proxy Set	Calls2Teams
SBC General	
Classify By Proxy Set	Enable
All other parameters can be left unchanged at their default values.	

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.



The screenshot shows the NEC SIP Manager interface. The left sidebar contains a 'TOPOLOGY VIEW' menu with options like 'CORE ENTITIES', 'CODERS & PROFILES', 'SBC', 'SIP DEFINITIONS', 'MESSAGE MANIPULATION', 'MESSAGE POLICIES', 'MEDIA', 'INTRUSION DETECTION', and 'SIP RECORDING'. The 'MESSAGE MANIPULATION' section is expanded, showing 'Message Conditions (2)', 'Message Policies (1)', and 'Pre-Parsing Manipulation Sets (0)'. The 'Message Conditions (2)' item is selected. The main area displays the 'Message Conditions' configuration page. The 'Name' field is set to 'Calls2Teams - User agent' and the 'Condition' field is set to 'header.User-Agent contains 'calls2Teams''. The 'Condition' field is highlighted with a red box. The 'Message Conditions' list on the right shows the configured 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.

The screenshot shows the NEC SBC Configuration interface. The left sidebar contains a tree view with categories like TOPOLOGY VIEW, CORE ENTITIES, CODERS & PROF, SBC, and MEDIA. The main area is titled 'Classification (3)'. It features two main sections: 'MATCH' and 'ACTION'. In the 'MATCH' section, the 'Name' field is set to 'Calls2Teams', 'Source SIP Interface' is '#1 [DMZ]', 'Source IP Address' is '40.69.2.153', and 'Message Condition' is '#0 [Calls2Teams - User agent]'. In the 'ACTION' section, the 'Action Type' is 'Allow', 'IP Group Selection' is 'Source IP Group', and 'Source IP Group' is '#2 [Calls2Teams IP Group]'. There are 'View' links next to several fields. At the bottom, there are 'Cancel' and 'APPLY' buttons.

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	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Terminate Options	Default_SBCRouting	Route Row	Any	OPTIONS	*	*	Dest Address	-	-	Internal
1	Calls2Teams > SV9100	Default_SBCRouting	Route Row	Calls2Teams IP Group	All	*	*	IP Group	SV9100 IP Group	-	-
2	SV9100 > Calls2Teams	Default_SBCRouting	Route Row	SV9100 IP Group	All	*	*	IP Group	Calls2Teams IP Group	-	-

#0[Terminate Options]

GENERAL

Name: Terminate Options

Alternative Route Options: Route Row

MATCH

Source IP Group: Any

Request Type: OPTIONS

Source Username Pattern: *

Source Host: *

Source Tag: *

Destination Username Pattern: *

Destination Host: *

Destination Tag: *

Message Condition: *

Call Trigger: Any

ReRoute IP Group: Any

ACTION

Destination Type: Dest Address

Destination IP Group: -

Destination SIP Interface: -

Destination Address: Internal

Destination Port: 0

Destination Transport Type: *

IP Group Set: -

Call Setup Rules Set ID: -1

Group Policy: Sequential

Cost Group: -

Routing Tag Name: default

Internal Action: *

Modified Destination User Name: *

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: SBCKEETORIGINALCALLID

Enter Value: 1

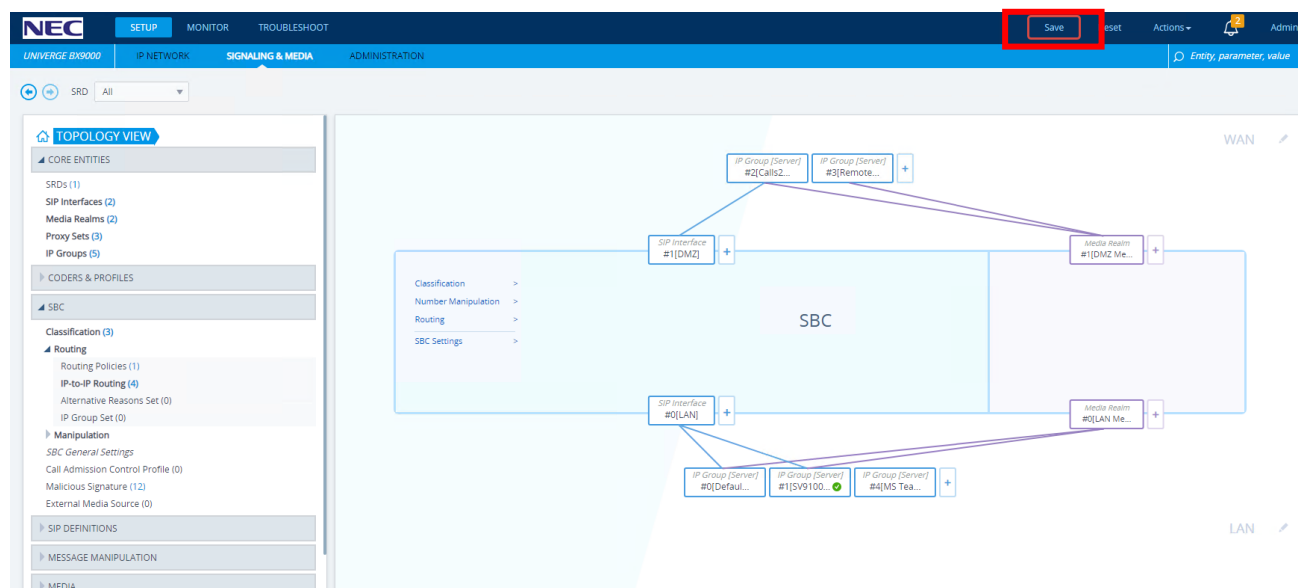
Apply New Value

Output Window

Parameter Name: SBCKEETORIGINALCALLID
Parameter New Value: 1
Parameter Description: SBC - Keep original call Id for outgoing messages

Parameter Name	Value
SBCKeepOriginalCallID	1

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

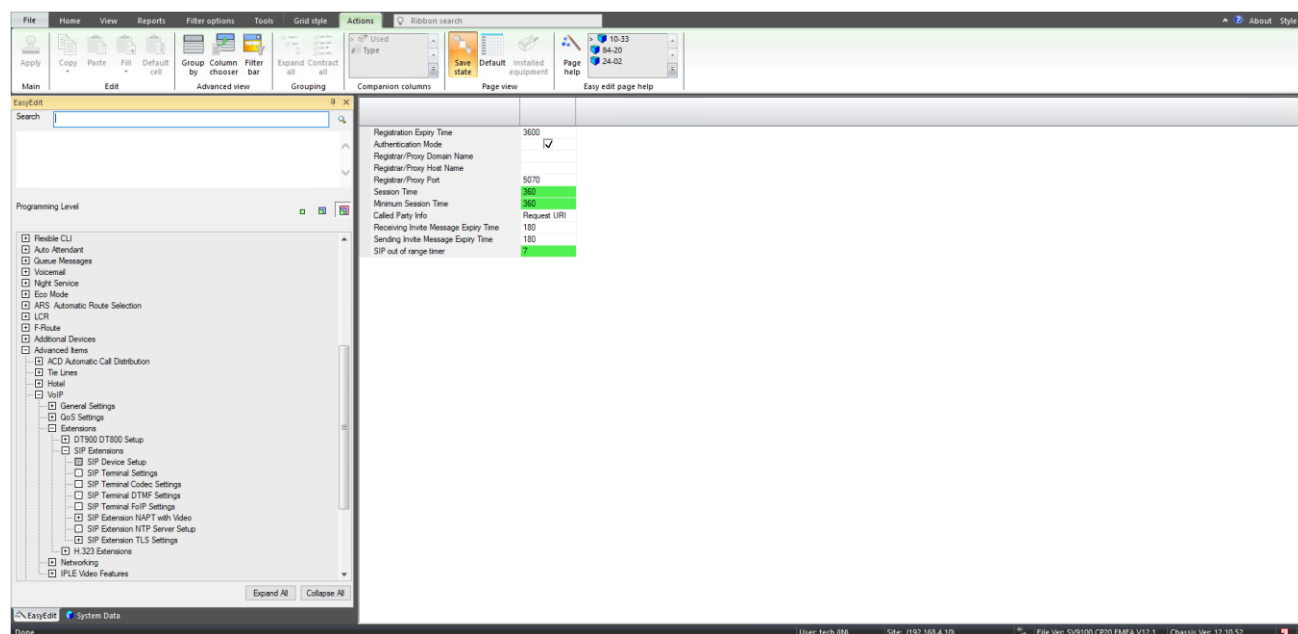


SV9100 Configuration

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*.

Station	Extension	Name	Peer to Peer Mode	Terminal Type	Terminal Type	Select Special Terminal Type	Terminal MAC Address	Nickname	Using IP Address	Codec Type	Authentication Password	IP duplication allow mode	Ac	trf
001	200	EXT 200	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
002	201	EXT 201	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
003	202	EXT 202	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
004	203	EXT 203	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
005	204	EXT 204	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
006	205	EXT 205	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
007	206	EXT 206	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
008	207	EXT 207	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
009	208	EXT 208	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
010	209	EXT 209	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
011	210	EXT 210	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
012	211	EXT 211	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
013	212	EXT 212	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
014	213	EXT 213	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
015	214	EXT 214	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
016	215	EXT 215	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
017	216	EXT 216	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
018	217	EXT 217	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
019	218	EXT 218	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
020	219	EXT 219	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
021	220	EXT 220	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
022	221	EXT 221	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
023	222	EXT 222	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
024	223	EXT 223	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
025	224	EXT 224	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
026	225	EXT 225	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
027	226	EXT 226	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		
028	227	EXT 227	On	None	Normal - Ignore DTMF tones	Fax	00-00-00-00-00-00	0.0.0.0	Type 1	Disable	Disable	Disable		

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

The screenshot shows the 'Calls2Teams' configuration wizard interface. At the top, there is a navigation bar with the 'Calls2Teams' logo and tabs for 'Getting Started', 'Services', 'Users', and 'Account'. The 'Getting Started' tab is active. Below the navigation bar, there is a progress bar with four steps: 'Prerequisites', 'PBX/Trunk', 'Teams', and 'Users'. The 'Prerequisites' step is currently selected and highlighted. The main content area is titled 'Welcome to the Call2Teams Wizard'. Below the title, there is a message: 'This wizard will help you setup your service and first user ready for calls. Before you begin the admin setup you will need:'. A list of prerequisites follows, each with a green checkmark to its right, indicating they are all met:

- A user/login to your Office 365 account with Global Admin rights.
- Microsoft Phone System licence add-ons (or E5 licences) for the end users of the service (not required if only using Phone App).
- One or two unassigned Office 365 user licenses such as Business Basic/Premium or E1/E3/E5, for a few hours during the initial setup.
- Access to your PBX or Trunk portal to create/manage SIP credentials.
- Using a modern compatible web browser.
- At least one Call2Teams license.
- Microsoft tenant supports Direct Routing configuration.

Below the list, there is a blue button labeled 'Check My Tenant' with a link 'View previous results' underneath it. At the bottom right, there is a blue button labeled 'Next'.

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

Call2Teams [Getting Started](#) [Services](#) [Users](#) [Account](#) [emea.nec.com](#) [?](#) [User](#)

[Prerequisites](#) **[PBX/Trunk](#)** [Teams](#) [Users](#)

[PBX](#) [Trunk](#)

Service Name *
 NEC SV9100

Country *
 United Kingdom

SIP Domain *

SIP Proxy

Authentication Type *
 Registration

PBX Source IPs
 IP Address 1.2.3.4

[+ Add Additional IP](#)

Calling Policy *
☒ Manage Teams Calling Policy

Teams Voicemail *
 Prohibit Voicemail

Music On Hold *
 PBX Hold Music

Expiry (seconds)

Protocol *
 TCP

Propagate Refer *
 PBX handles transfers

Suppress Contact Data Param *
 Yes

Encrypt Media *
 No

Override Codes *
 Pass Through All Codes

Outside Line Prefix
 9

E164 Number Format
 Localized

E164 Number Translation
 This PBX's country is configured as United Kingdom which has a dialing country code of 44

Outbound International Prefix
 00

Outbound National Prefix
 0

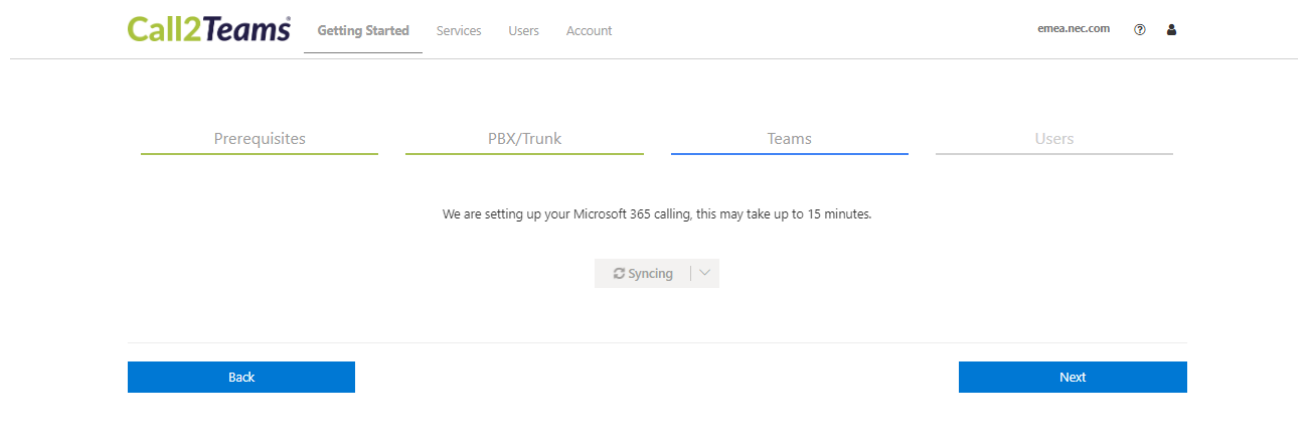
Inbound International Prefix
 00

Inbound National Prefix
 0

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.



- 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.

This form will connect your PBX/Trunk user with a specific Teams user.

Teams

Select a User

Calls2teams 2 (Calls2teams2@52s7zp.onmicrosoft.com)

▼

Phone Number (United Kingdom)

+44 1157778552

Calling Policy

☐ Override Teams Calling Policy

NEC SV9100

SIP Username *

227 @82.12.39.59

Auth Username

227

Password

.....

Add User and Sync

Back

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.

Congratulations, your service is now ready for calling.

Users

22 of 25 PBX and 25 of 25 Trunk and 50 of 50 Phone App user licences available.

Syncing

[Add User](#) [Import Users](#)

User	Service Type	SIP User	Registration	Calls
			All	
▶ Calls2teams 1	Standard User	226	●	↕
▶ Calls2teams 2	Standard User	227	●	↕

- 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.

Congratulations, your service is now ready for calling.

Users

22 of 25 PBX and 25 of 25 Trunk and 50 of 50 Phone App user licences available.

Syncing

[Add User](#) [Import Users](#)

Service: NEC SV9100

Import Type: Create

CSV File: Choose File

No file chosen

Download CSV Template

Cancel Upload

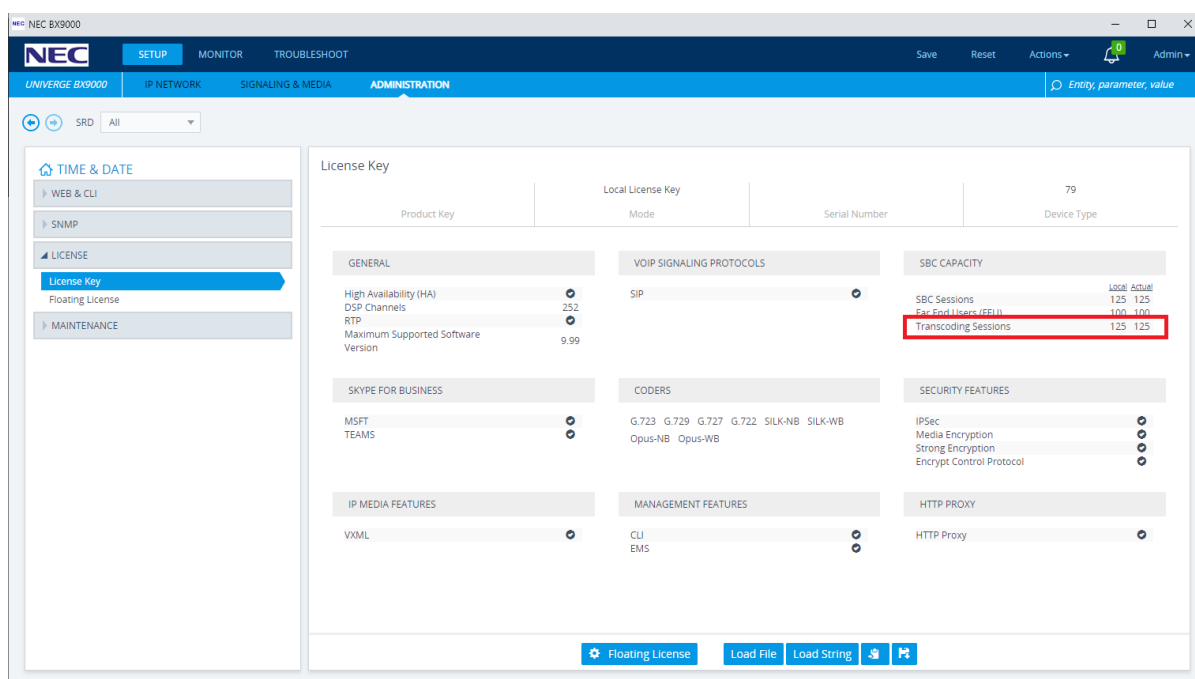
User	Service Type	SIP User	Registration	Calls
			All	
▶ Calls2teams 1	Standard User	226	●	↕
▶ Calls2teams 2	Standard User	227	●	↕

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).

NEC BX9000

UNIVERGE BX9000

SIGNALING & MEDIA

Media Settings

GENERAL

NAT Traversal: Disable NAT

Enable Continuity Tones: Disable

Number of Media Channels: 120

Enforce Media Order: Disable

SDP Session Owner: UNIVERGEBX9000

ROBUSTNESS

Inbound Media Latch Mode: Dynamic

New RTP Stream Packets: 3

New RTCP Stream Packets: 3

New SRTP Stream Packets: 3

New SRTP Stream Packets: 3

Timeout To Relatch RTP (msec): 200

Timeout To Relatch SRTP (msec): 200

Timeout To Relatch Silence (msec): 10000

Timeout To Relatch RTCP (msec): 10000

SBC SETTINGS

Preferences Mode: Doesn't Include Extensions

Enforce Media Order: Disable

Cancel APPLY

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

NEC BX9000

UNIVERGE BX9000

SIGNALING & MEDIA

SBC General Settings

GENERAL

Direct Media: Disable

Unclassified Calls: Reject

Forking Handling Mode: Latch On First

No Answer Timeout [sec]: 600

BroadWorks Survivability Feature: Disable

Max Forwards Limit: 70

Max Call Duration [min]: 0

No RTP Timeout After Connect [ms]: 0

Keep original user in Register: Do not keep user; Override wit

SBC Performance Profile: Optimized for transcoding

Routing Timeout [sec]: 10

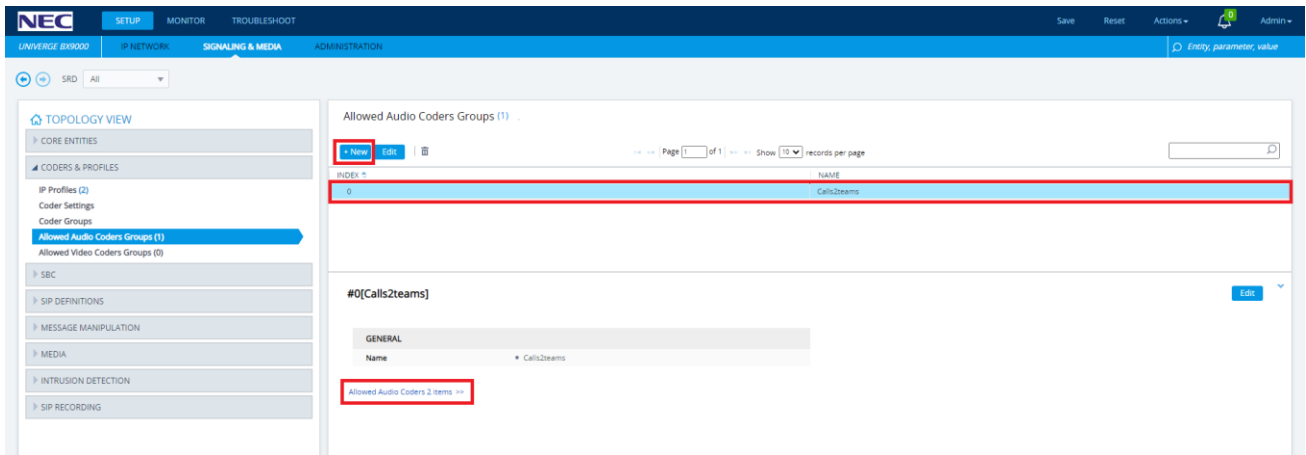
Call duration that counts as a short call: 2

FORWARD & TRANSFER

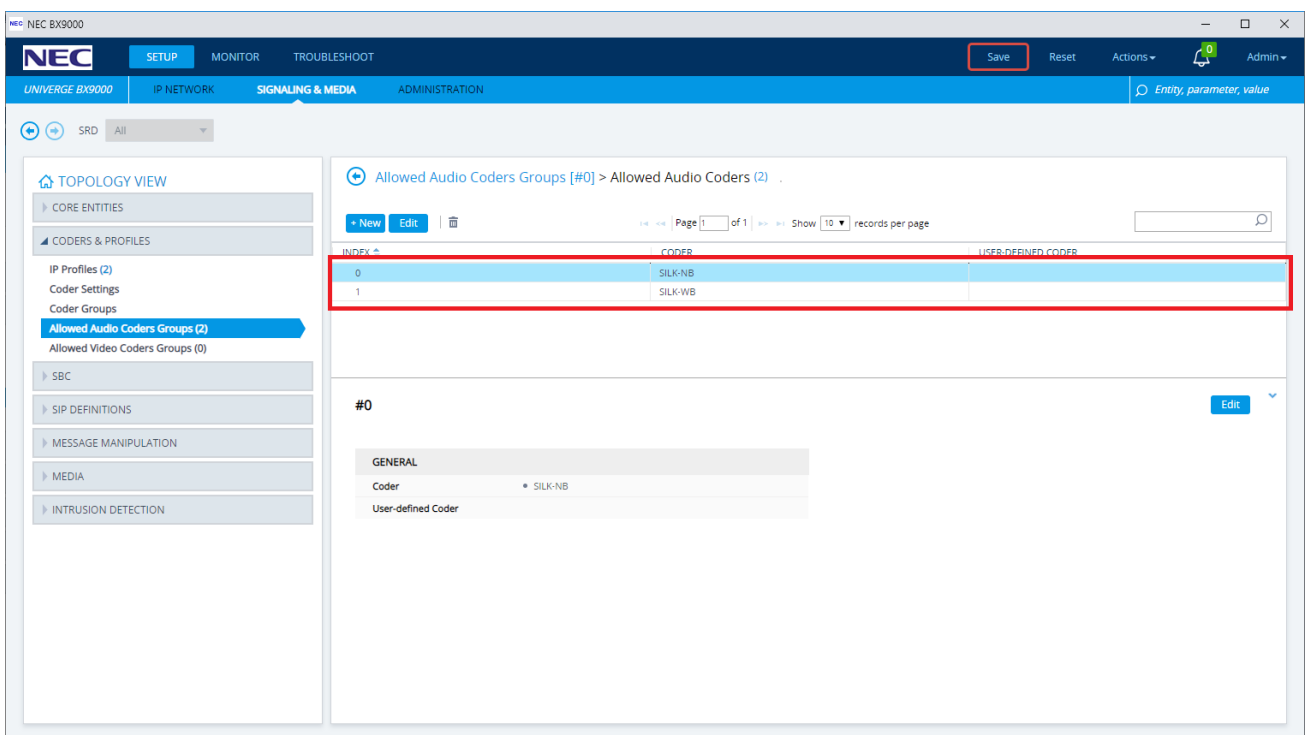
SBC REFER Behavior: Regular

Cancel APPLY

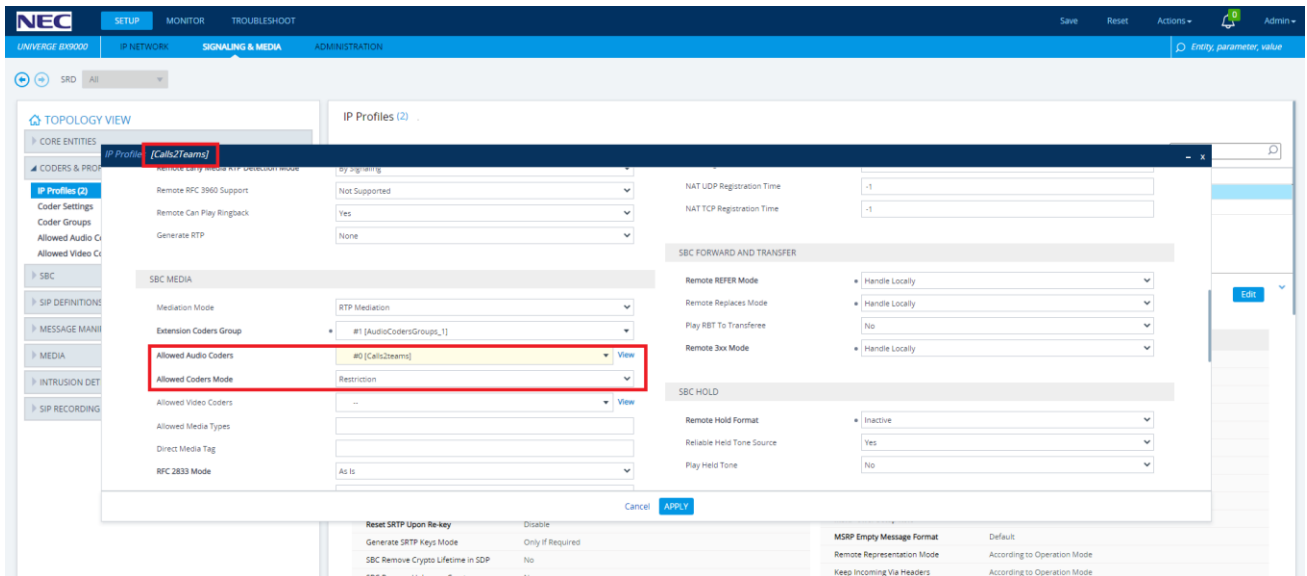
4. Create an 'Allowed' coder group for Calls2Teams in *SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Allowed Audio Coders Groups*. Open the child table.



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=155627] [SID=21916f:114:5051] (N 142865) ConnectionData:CalculateResourcesForExtTranscoding Leading:DSP Opposite:CODERTRANSCODING MediationLevel:RTP [Time:15-02@23:06:26.119]
192.168.88.5 local0.notice [S=155628] [SID=21916f:114:5051] (N 142865) ResourceCounter: Code Transcoding session +1 [17/120] [Time:15-02@23:06:26.119]
192.168.88.5 local0.notice [S=155629] [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=155630] [SID=21916f:114:5051] (N 142867) ResourceCounter: add channelResource:AllocateResource DSP Allocated Available count 1021 [Time:15-02@23:06:26.119]
192.168.88.5 local0.notice [S=155631] [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=155632] [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=155633] [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.

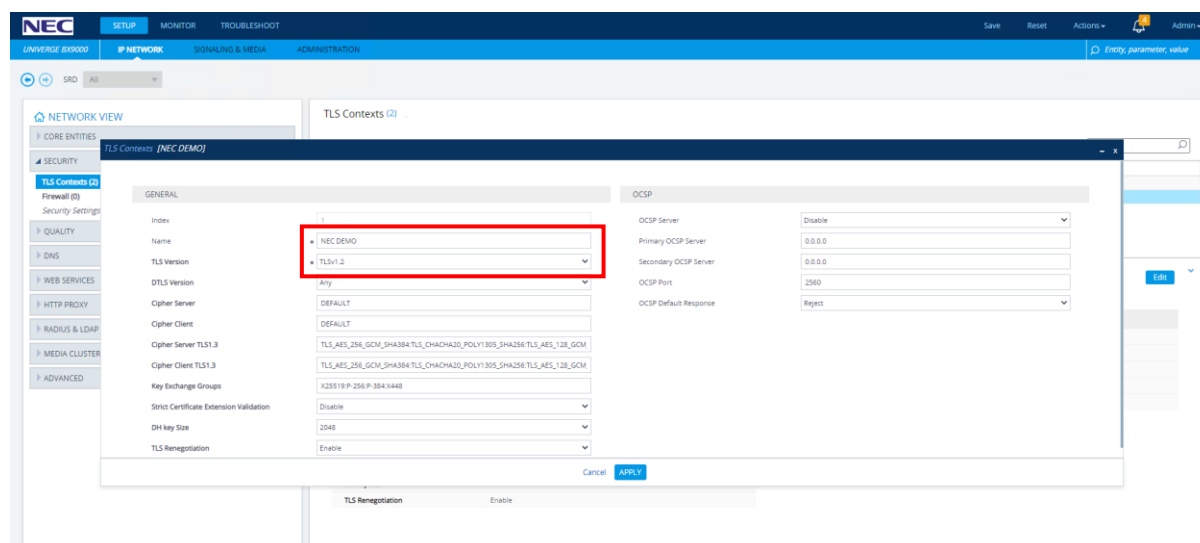
Configure your TLS Context

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.

NEC BX9000

NEC SETUP MONITOR TROUBLESHOOT Save Reset Actions Admin

UNIVERGE BX9000 IP NETWORK SIGNALING & MEDIA ADMINISTRATION Entity, parameter, value

SRD All

NETWORK VIEW

- CORE ENTITIES
- SECURITY
 - TLS Contexts (1)**
 - Firewall (0)
 - Security Settings
- QUALITY
- DNS
- WEB SERVICES
- HTTP PROXY
- RADIUS & LDAP
- MEDIA CLUSTER
- ADVANCED

TLS Contexts (1)

+ New Edit Show 10 records per page

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	NECDemo	TLSv1.2	Any	HIGH

#0[NECDemo] Edit

GENERAL		OCSP	
Name	NECDemo	OCSP Server	Disable
TLS Version	TLSv1.2	Primary OCSP Server	0.0.0.0
DTLS Version	Any	Secondary OCSP Server	0.0.0.0
Cipher Server	HIGH	OCSP Port	2560
Cipher Client	HIGH	OCSP Default Response	Reject
Strict Certificate Extension	Disable		
DH key Size	1024		
TLS Renegotiation	Enable		

Certificate Information >> Change Certificate >> Trusted Root Certificates >>

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

⊕ TLS Context [#1] > Certificate Information

PRIVATE KEY

Key size: 2048 bits
Status: OK

CERTIFICATE

Certificate:

Data:

Version: 3 (0x2)
Serial Number:
c2:26:57:c3:1e:91:ae:38
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
Validity
Not Before: Jan 21 13:58:07 2022 GMT
Not After : Feb 22 13:58:07 2023 GMT
Subject: CN=*.necdemo.co.uk

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

00:b5:7b:40:9a:a8:66:15:f7:50:13:d4:5d:6b:6f:
e7:8f:94:b9:b6:cd:a1:72:c9:50:44:88:56:70:75:
a6:5d:70:9c:5b:88:22:6a:d3:e3:24:78:18:dd:f3:
2f:84:68:3c:75:b4:52:ad:cd:3a:a5:b4:47:a2:03:
54:e0:af:23:75:8b:7f:95:80:c7:5a:ed:5d:d7:87:
bd:a6:ec:f8:2f:8f:b1:50:a7:8c:d0:c5:d5:14:e3:
f0:d8:5e:fb:aa:aa:4e:18:18:92:8c:1b:a6:07:c8:
b5:6a:eb:38:39:59:dc:e8:df:16:ea:8a:1b:e8:ce:
31:c5:d9:79:bb:69:6f:16:7c:d4:af:09:36:c0:26:
3f:a8:e1:84:fe:16:c2:2a:be:6a:2c:e8:bf:35:df:
37:08:b5:c6:71:5c:55:93:c1:27:38:2f:b0:d4:8c:
12:29:ab:82:04:dc:3b:21:5c:d7:75:bc:72:bc:46:
8a:a5:5e:ed:1f:63:28:cc:0c:13:60:ff:59:56:18:
ea:61:66:3d:e7:fe:8d:78:81:c9:a2:f3:74:60:
47:af:b9:b3:d4:db:d4:38:f5:68:a7:de:ac:ad:89:
cd:ca:db:95:11:33:b0:23:a4:0a:1e:be:10:00:3d:
b4:43:ea:a8:73:31:e2:f2:f8:06:f5:e5:66:22:39:
...

- 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.

NEC UNIVERGE BX9000

SETUP MONITOR TROUBLESHOOT

UNIVERGE BX9000 IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Entity, parameter, value

SRD All

NETWORK VIEW

CORE ENTITIES

SECURITY

TLS Contexts (1)

Firewall (0)

Security Settings

QUALITY

DNS

WEB SERVICES

HTTP PROXY

RADIUS & LDAP

MEDIA CLUSTER

ADVANCED

TLS Context [#0] > Trusted Root Certificates

View Import Export Remove

INDEX	SUBJECT	ISSUER	EXPIRES
0	Go Daddy Secure Certificate Aut	Go Daddy Root Certificate Autho	5/03/2031
1	Go Daddy Root Certificate Autho	Go Daddy Root Certificate Autho	12/31/2037
2	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025

Page 1 of 1 10 View 1 - 3 of 3

Selected Row #0

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 7 (0x7)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2

Validity

Not Before: May 3 07:00:00 2011 GMT

Not After: May 3 07:00:00 2031 GMT

Subject: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public Key: (2048 bit)

Modulus:

00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
b8:81:08:6c:c3:04:d9:62:17:8e:2f:3e:65:cf:
8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
63:83:62:90:ce:f1:69:6c:99:c8:1a:14:8b:4c:cc:
45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:

- 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.

NEC UNIVERGE BX9000

SETUP MONITOR TROUBLESHOOT

UNIVERGE BX9000 IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Entity, parameter, value

SRD All

TOPOLOGY VIEW

CORE ENTITIES

SIP Interfaces (2)

Media Realms (2)

Proxy Sets (3)

IP Groups (5)

CODERS & PROF

SBC

Classification (3)

Routing

Routing Policy

IP-to-IP Route

Alternative R

IP Group Set

Manipulation

SBC General Set

Call Admission C

Malicious Signat

External Media S

SIP DEFINITION

MESSAGE MAN

MEDIA

INTRUSION DETECTION

SIP RECORDING

SIP Interfaces (2)

SRD #0 [DefaultSRD]

GENERAL

Index 1

Name DMZ

Topology Location Up

Network Interface #1 [DMZ]

Application Type SBC

UDP Port 0

TCP Port 0

TLS Port 5071

SCTP Port 0

SCTP Secondary Network Interface --

MEDIA

Media Realm #1 [DMZ Media Realm]

Direct Media Disable

SECURITY

TLS Context Name #1 [NEC DEMO]

TLS Mutual Authentication --

Message Policy --

User Security Mode Not Configured

Enable Un-Authenticated Registrations Not configured

Max. Number of Registered Users 1

Additional UDP Ports

Additional UDP Ports Mode Always Open

Encapsulating Protocol No encapsulation

Enable TCP Keepalive Disable

Used By Routing Server Not Used

Pre-Parsing Manipulation Set --

CAC Profile --

Cancel APPLY

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.

Service Name: NEC SV9100 Country: United Kingdom

SIP Domain: jpllab.necdemo.co.uk SIP Proxy: jpllab.necdemo.co.uk:5077

Authentication Type: Registration PBX Source IPs: 1.2.3.4

+ Add Additional IP

Calling Policy: ☒ Manage Teams Calling Policy

Teams Voicemail: Prohibit Voicemail Music On Hold: PBX Hold Music

Expiry (seconds): 360 Protocol: TLS Propagate Refer: PBX handles transfers Suppress Contact Data Param: Yes

Encrypt Media: No Override Codecs: Pass Through All Codecs

Outside Line Prefix: 9 E164 Number Format: Localized

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.

NEC SETUP MONITOR TROUBLESHOOT

UNIVERGE B89000 IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions Admin

Entity, parameter, value

SRD: All

TOPOLOGY VIEW

CORE ENTITIES

SRDs (1)

SIP Interfaces (2)

Media Realms (2)

Proxy Sets (2)

IP Groups (5)

CODES & PROFILES

SBC

Classification (3)

Routing

Routing Policies (1)

IP-to-IP Routing (4)

Alternative Reasons Set (0)

IP Group Set (0)

Manipulation

SBC General Settings

Call Admission Control Profile (0)

Malicious Signature (1)

External Media Source (0)

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

Proxy Sets (#2) > Proxy Address (2)

Page 1 of 1 Show 15 records per page

INDEX	PROXY ADDRESS	TRANSPORT TYPE
0	40.89.2.153:8002	TLS
1	20.136.150.164:8002	TLS

Proxy Address

#0

GENERAL

Index: 0

Proxy Address: 40.89.2.153:8002

Transport Type: TLS

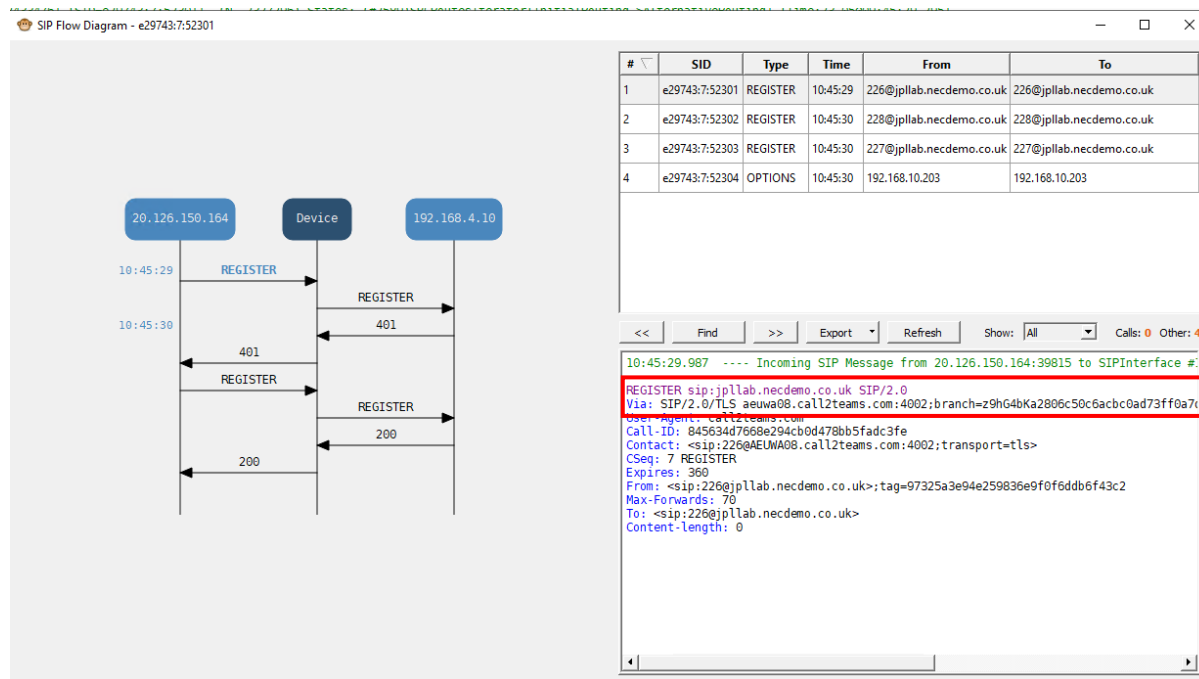
Proxy P: 1

Proxy R: 1

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
<input type="text"/>		<input type="text"/>	All <input type="button" value="v"/>	
▶ Calls2teams 1	Standard User	226	<div><div></div></div>	<div><div></div><div></div></div>
▶ Kit 2	Standard User	228	<div><div></div></div>	<div><div></div><div></div></div>
▶ Calls2teams 2	Standard User	227	<div><div></div></div>	<div><div></div><div></div></div>

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 3 rd 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