Ribbon EdgeMarc Teams Direct Routing Configuration

Prakash Kothandaraman

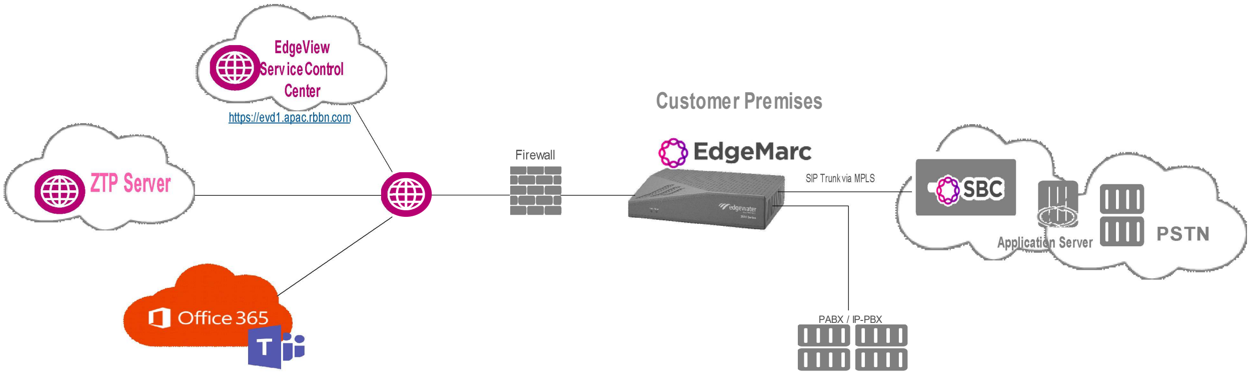
Ribbon EdgeMarc Teams-DR Configuration

Table of Contents

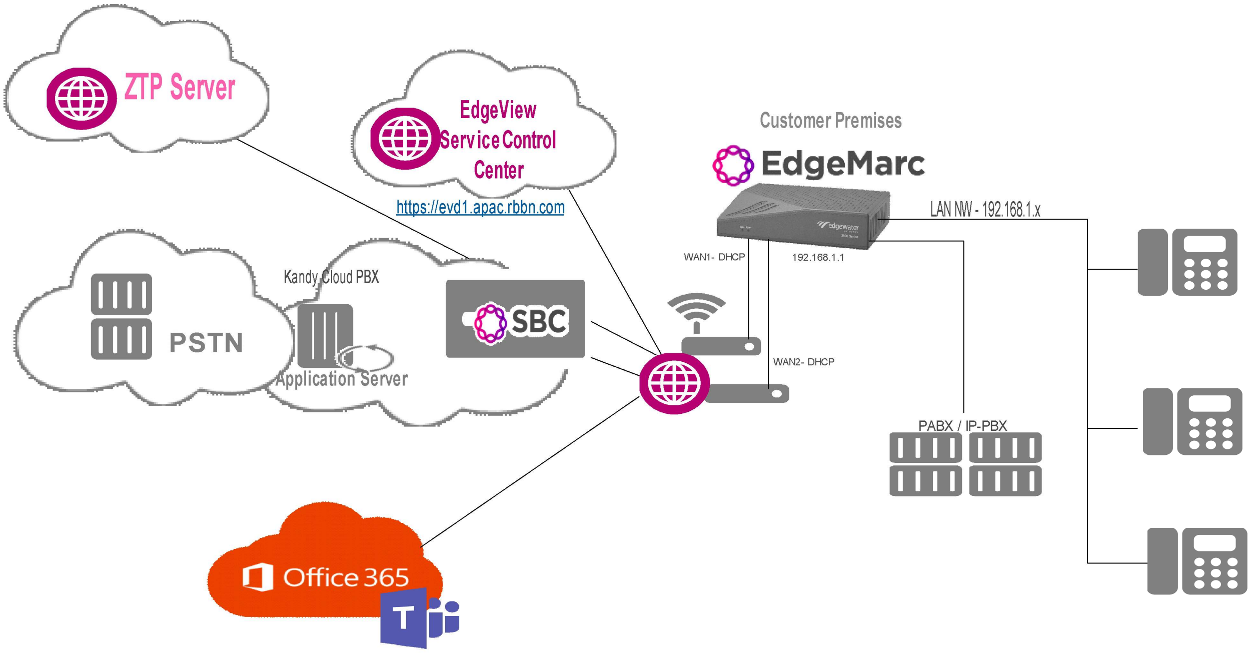
Ribbon EdgeMarc Teams-DR Configuration

Teams DR- Network Topology:

Teams Direct Routing- EdgeMarc Deployment #1:



Teams Direct Routing- EdgeMarc Deployment #2:



Ribbon EdgeMarc Teams-DR Configuration

Pre-requisite:

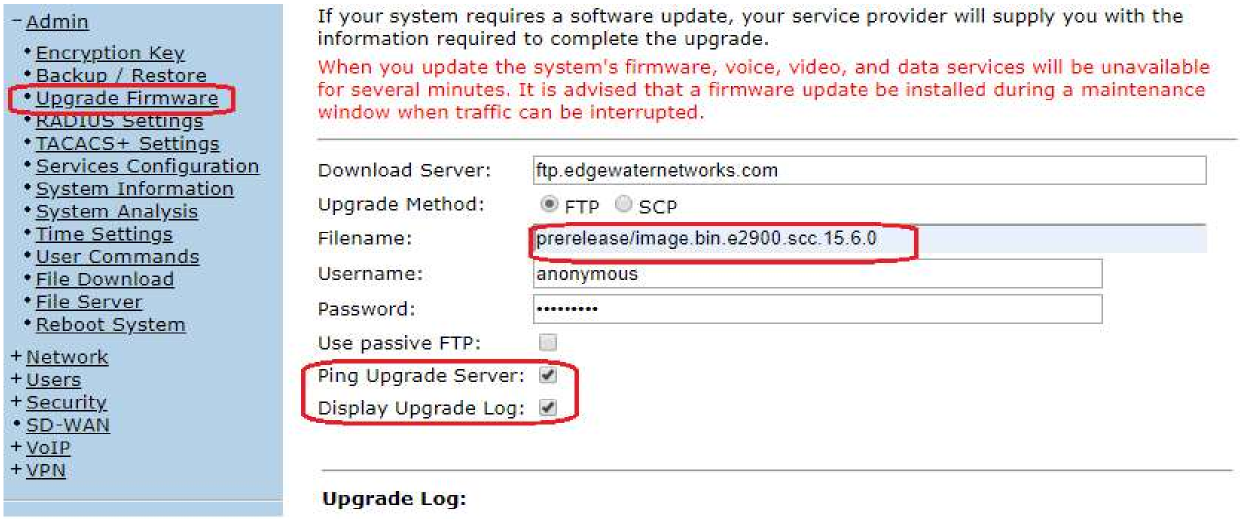
- EdgeMarc firmware version – 15.6.0 or above
- Public FQDN for Teams Tenant - Teams PSTN Gateway (EdgeMarc)
- The public IP address for Teams Tenant - Teams PSTN Gateway (EdgeMarc)
- Signed SSL certificate by CA
- CA Root certificate and intermediate cert (if any)
- MS Teams Admin account with E3 or E5 license
- PSTN Break via SIP Trunk or TDM (EM with PRI model – 4xxx series)

EdgeMarc Firmware Upgrade

Ensure EdgeMarc is upgraded to firmware version 15.6 or above release version before performing Teams Direct Routing configuration.

Login to EdgeMarc.
192.168.1.1 (default LAN IP) – root/default (First time login password)

Admin →Upgrade Firmware



If your system requires a software update, your service provider will supply you with the information required to complete the upgrade.

When you update the system's firmware, voice, video, and data services will be unavailable for several minutes. It is advised that a firmware update be installed during a maintenance window when traffic can be interrupted.

Download Server:	ftp.edgewaternetworks.com
Upgrade Method:	● FTP ○ SCP
Filename:	prerelease/image.bin.e2900.scc.15.6.0
Username:	anonymous
Password:	•••••••••
Use passive FTP:	□
Ping Upgrade Server:	☑
Display Upgrade Log:	☑

Upgrade Log:

Click Upgrade, wait for 5-10 minutes for upgrade to complete

Note: Ensure Filename has right EdgeMarc Model

prerelease/image.bin.e2900.ewn.15.6.0 << for EM2900e with Perpetual License
prerelease/image.bin.e2900.scc.15.6.0 << for EM2900e with Subscription License
prerelease/image.bin.e4808.ewn.15.6.0 << for EM4808 with Perpetual License
prerelease/image.bin.e4808.scc.15.6.0 << for EM4808 with Subscription License
prerelease/image.bin.e4808v2.ewn.15.6.0 << for EM4808 GW model with Perpetual License
prerelease/image.bin.e4808v2.scc.15.6.0 << for EM4808 GW model with Subscription License

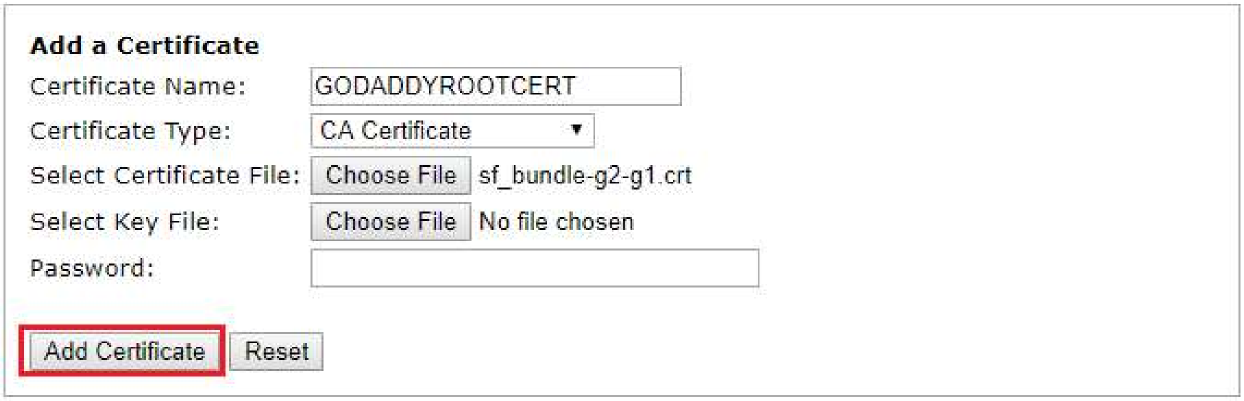
Generate CSR:

Refer to appendix section for CSR generation and Certificate options

Upload SSL Certificate:

Add CA Cert to EdgeMarc

Add all root, intermediate certificate, choose certificate Type as CA Certificate



Add a Certificate

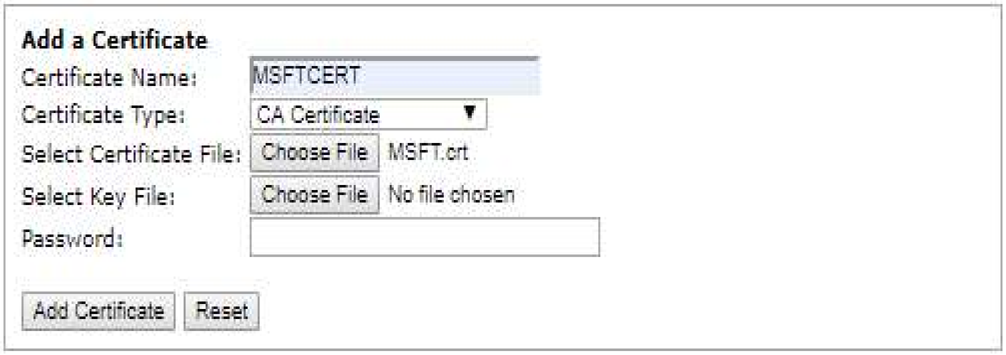
Certificate Name:	GODADDYROOTCERT
Certificate Type:	CA Certificate ▾
Select Certificate File:	Choose File sf_bundle-g2-g1.crt
Select Key File:	Choose File No file chosen
Password:	

Similarly, add intermediate certs if any available.

Add MSFT Baltimore cert to EdgeMarc

Add Microsoft Teams Baltimore certificate, choose certificate Type as CA Certificate

Cert available - https://cacert.omniroot.com/bc2025.crt

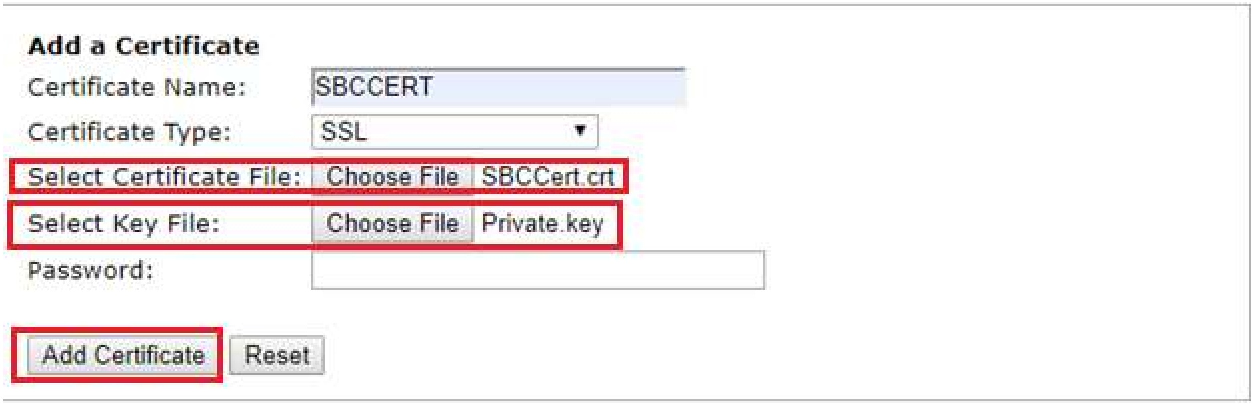


Add a Certificate

Certificate Name:	MSFTCERT
Certificate Type:	CA Certificate ▾
Select Certificate File:	Choose File MSFT.crt
Select Key File:	Choose File No file chosen
Password:	

Add SBC Cert to EdgeMarc

Add SBC SSL cert, choose certificate Type as SSL



Add a Certificate

Certificate Name: SBCCERT

Certificate Type: SSL

Select Certificate File: Choose File SBCCert.crt

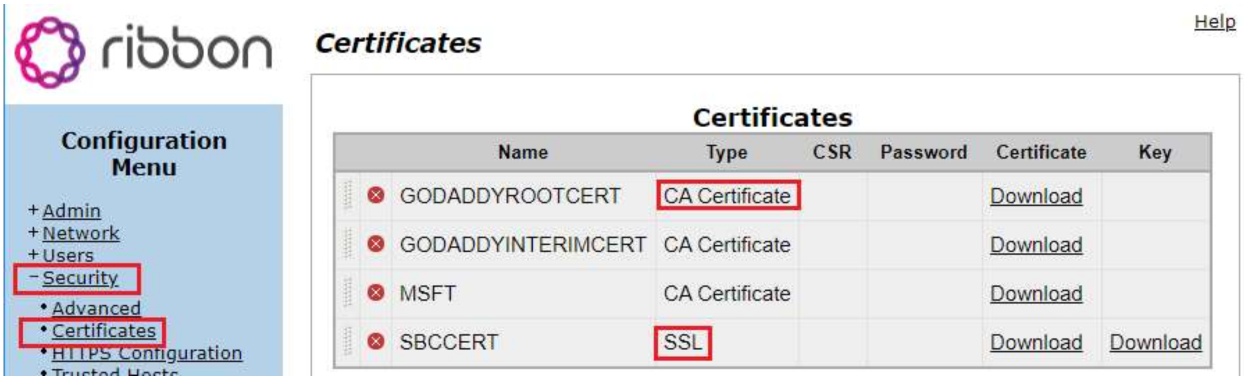
Select Key File: Choose File Private.key

Password:

Finally click on submit under the same page, wait for EM to load the certs

Once EM loads the SSL cert, you can view on certificate page.

Verify the upload of the cert



Certificates

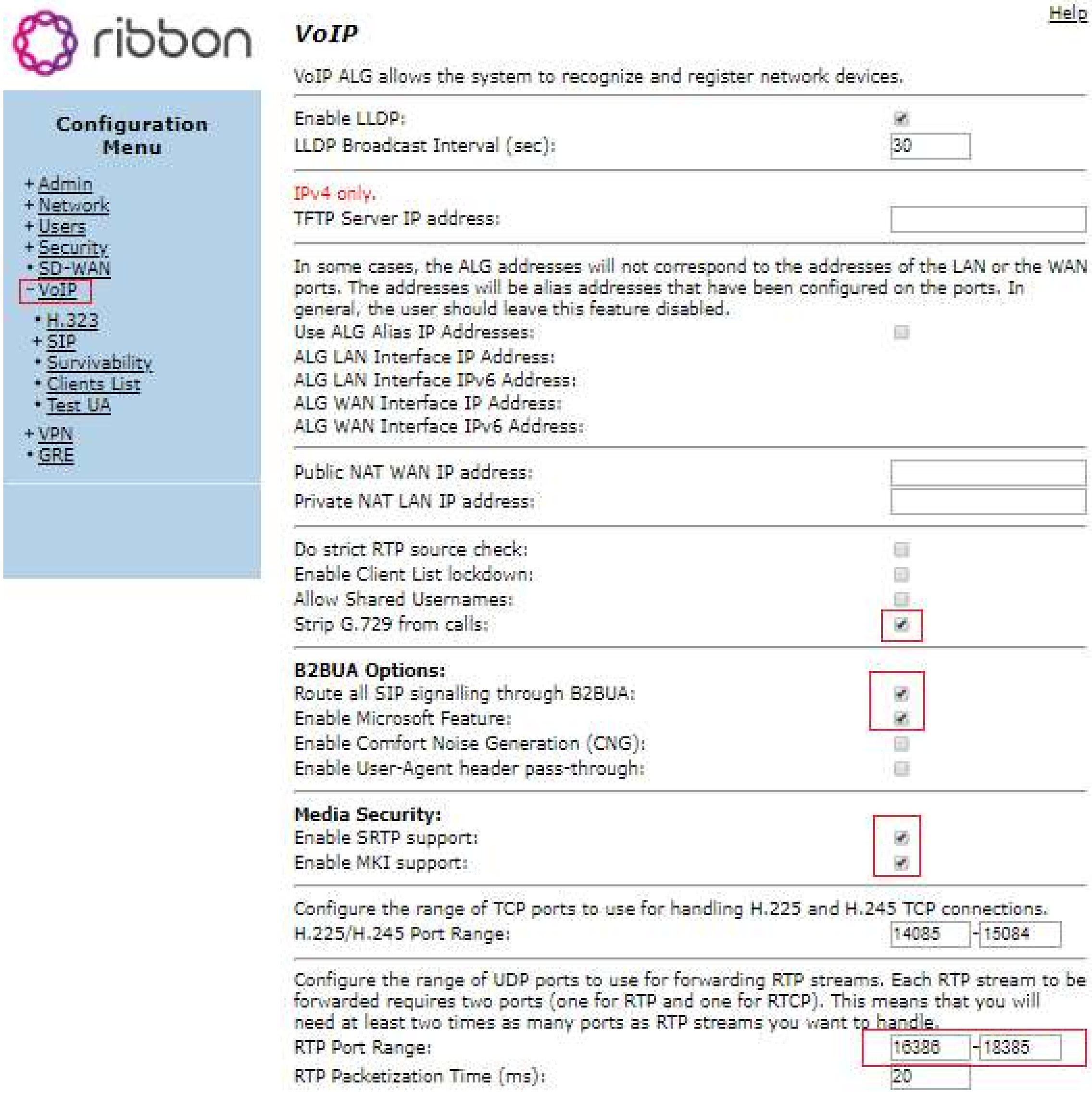
Certificates

Name	Type	CSR	Password	Certificate	Key
GODADDYROOTCERT	CA Certificate			Download	
GODADDYINTERIMCERT	CA Certificate			Download	
MSFT	CA Certificate			Download	
SBCCERT	SSL			Download	Download

Ribbon EdgeMarc Teams-DR Configuration

VOIP Configuration:

- Enable B2BUA Routing
- Enable Microsoft Feature
- Enable SRTP on Media Security
- Enable MKI Support
- Strip G.729 from Calls



VoIP

VoIP ALG allows the system to recognize and register network devices.

Enable LLDP: ☑
LLDP Broadcast Interval (sec): 30

IPv4 only.
TFTP Server IP address:

In some cases, the ALG addresses will not correspond to the addresses of the LAN or the WAN ports. The addresses will be alias addresses that have been configured on the ports. In general, the user should leave this feature disabled.

Use ALG Alias IP Addresses: ☐
ALG LAN Interface IP Address:
ALG LAN Interface IPv6 Address:
ALG WAN Interface IP Address:
ALG WAN Interface IPv6 Address:

Public NAT WAN IP address:
Private NAT LAN IP address:

Do strict RTP source check: ☐
Enable Client List lockdown: ☐
Allow Shared Usernames: ☐
Strip G.729 from calls: ☑

B2BUA Options:
Route all SIP signalling through B2BUA: ☑
Enable Microsoft Feature: ☑
Enable Comfort Noise Generation (CNG): ☐
Enable User-Agent header pass-through: ☐

Media Security:
Enable SRTP support: ☑
Enable MKI support: ☑

Configure the range of TCP ports to use for handling H.225 and H.245 TCP connections.
H.225/H.245 Port Range: 14085 - 15084

Configure the range of UDP ports to use for forwarding RTP streams. Each RTP stream to be forwarded requires two ports (one for RTP and one for RTCP). This means that you will need at least two times as many ports as RTP streams you want to handle.
RTP Port Range: 16386 - 18385
RTP Packetization Time (ms): 20

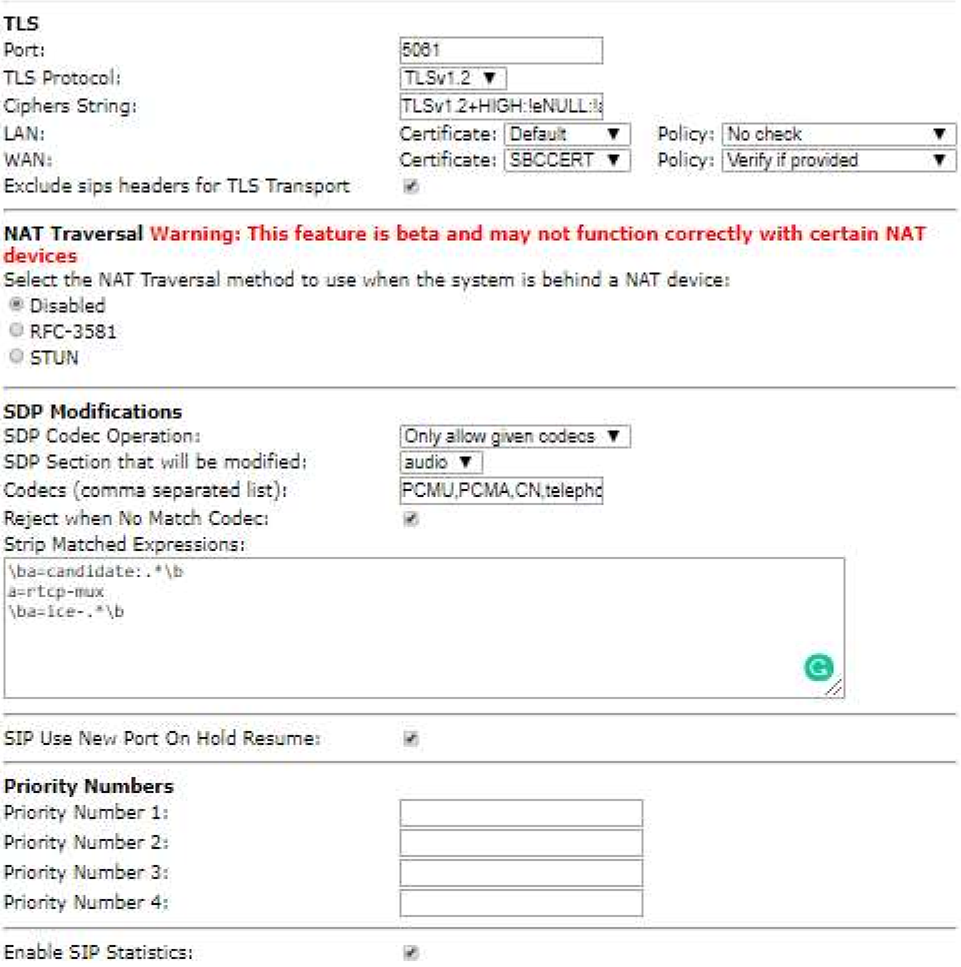
SIP SDP Configuration:

Go to VOIP → SIP

- SDP Codec operation: only allow given codecs
- SDP Section that will be modified: audio
- Codecs: PCMU,PCMA,CN,telephone-event
- Strip Matched express: \ba=candidate:.*\b

a=rtcp-mux

\ba=ice-.*\b



TLS

Port:	5061	
TLS Protocol:	TLSv1.2 ▼	
Ciphers String:	TLSv1.2+HIGH:!eNULL:!	
LAN:	Certificate: Default ▼	Policy: No check ▼
WAN:	Certificate: SBCCERT ▼	Policy: Verify if provided ▼
Exclude sips headers for TLS Transport	☑	

NAT Traversal **Warning: This feature is beta and may not function correctly with certain NAT devices**

Select the NAT Traversal method to use when the system is behind a NAT device:

● Disabled
○ RFC-3581
○ STUN

SDP Modifications

SDP Codec Operation:	Only allow given codecs ▼
SDP Section that will be modified:	audio ▼
Codecs (comma separated list):	PCMU,PCMA,CN,telepho
Reject when No Match Codec:	☑

Strip Matched Expressions:

```
\ba=candidate:.*\b
a=rtcp-mux
\ba=ice-.*\b
```

SIP Use New Port On Hold Resume:	☑

Priority Numbers

Priority Number 1:	
Priority Number 2:	
Priority Number 3:	
Priority Number 4:	

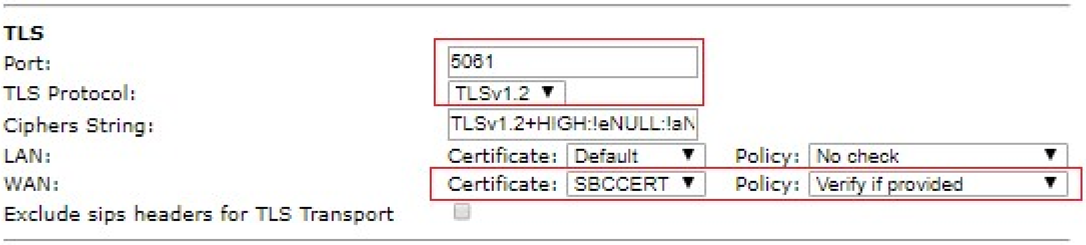
Enable SIP Statistics:	☑

Ribbon EdgeMarc Teams-DR Configuration

SIP TLS Configuration:

Go to VOIP → SIP

- Configure TLS port for MSFT Teams interface
- Choose the TLS Protocol version – TLS 1.2
- On WAN interface choose SBC Certificate and enable policy “Verify if provided”



TLS

Port: 5061

TLS Protocol: TLSv1.2 ▼

Ciphers String: TLSv1.2+HIGH:!eNULL:!aN

LAN: Certificate: Default ▼ Policy: No check ▼

WAN: Certificate: SBCCERT ▼ Policy: Verify if provided ▼

Exclude sips headers for TLS Transport □

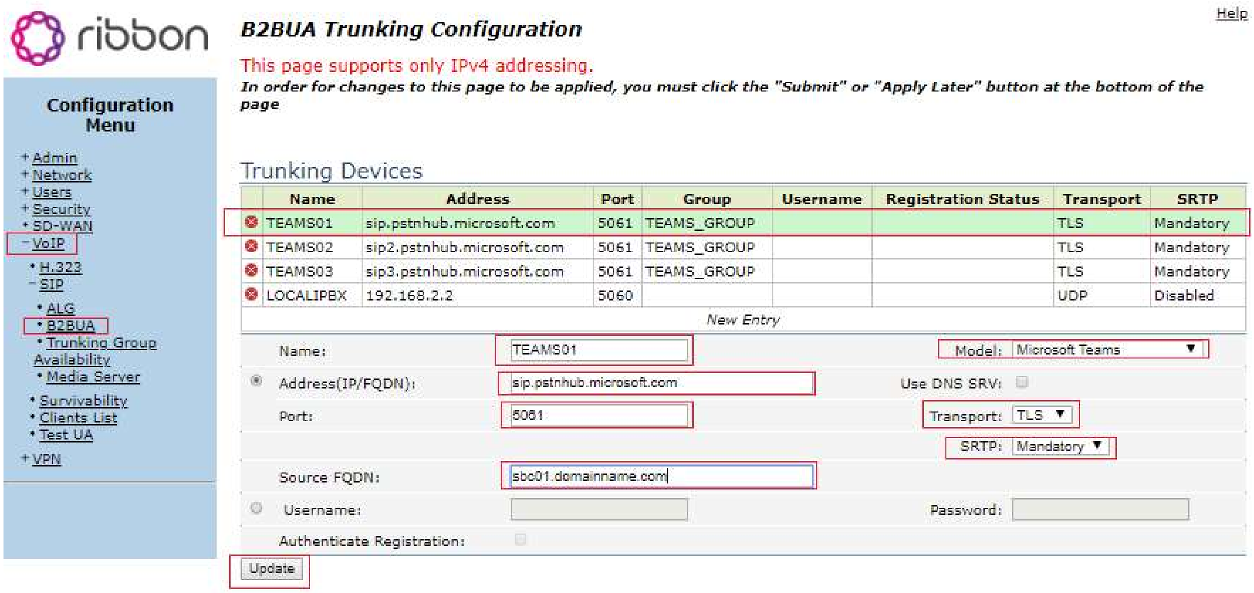
B2BUA Configuration:

Add Trunking Device Configuration:

Go to VOIP → SIP → B2BUA → Trunking Devices

Add Teams PBX Trunking configuration as shown below

- Add Trunking device for Primary, Secondary Territory Teams PBX server.
- Choose PBX Model as Microsoft Teams
- Choose SRTP on Media Security
- Choose TLS on Signaling Encryption



B2BUA Trunking Configuration

This page supports only IPv4 addressing.

In order for changes to this page to be applied, you must click the "Submit" or "Apply Later" button at the bottom of the page

Trunking Devices

	Name	Address	Port	Group	Username	Registration Status	Transport	SRTP
⊗	TEAMS01	sip.pstnhub.microsoft.com	5061	TEAMS_GROUP			TLS	Mandatory
⊗	TEAMS02	sip2.pstnhub.microsoft.com	5061	TEAMS_GROUP			TLS	Mandatory
⊗	TEAMS03	sip3.pstnhub.microsoft.com	5061	TEAMS_GROUP			TLS	Mandatory
⊗	LOCALIPBX	192.168.2.2	5060				UDP	Disabled

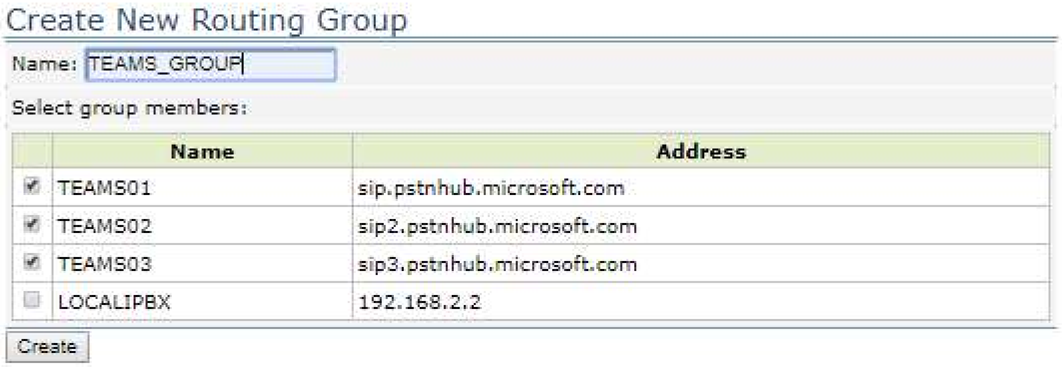
New Entry

	Name:	TEAMS01	Model:	Microsoft Teams ▼
●	Address(IP/FQDN):	sip.pstnhub.microsoft.com	Use DNS SRV:	□
	Port:	5061	Transport:	TLS ▼
			SRTP:	Mandatory ▼
	Source FQDN:	sbc01.domainname.com		
○	Username:		Password:	
	Authenticate Registration:	□		

Ribbon EdgeMarc Teams-DR Configuration

Create a Routing Group:

Create Routing Group configuration to handle the Teams Failover mechanism.



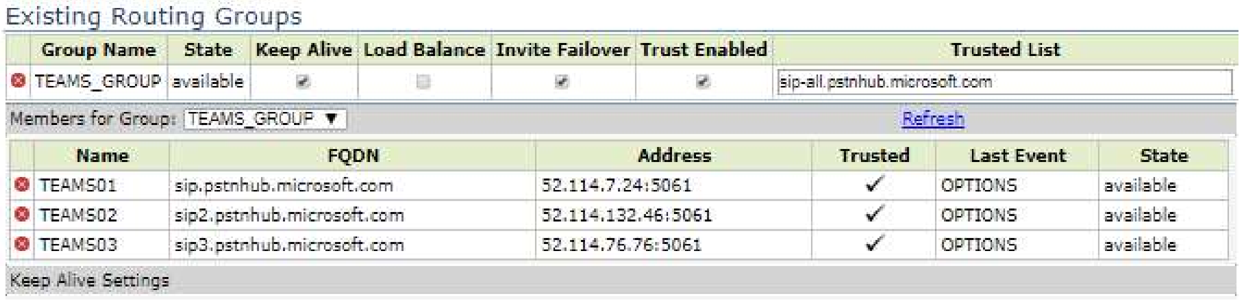
Create New Routing Group

Name: TEAMS_GROUP

Select group members:

	Name	Address
☑	TEAMS01	sip.pstnhub.microsoft.com
☑	TEAMS02	sip2.pstnhub.microsoft.com
☑	TEAMS03	sip3.pstnhub.microsoft.com
□	LOCALIPBX	192.168.2.2

- Enable Keep-Alive
- Enable Trusted list
- Enable Invite Failover



Existing Routing Groups

	Group Name	State	Keep Alive	Load Balance	Invite Failover	Trust Enabled	Trusted List
⊗	TEAMS_GROUP	available	☑	□	☑	☑	sip-all.pstnhub.microsoft.com

Members for Group: TEAMS_GROUP ▼

	Name	FQDN	Address	Trusted	Last Event	State
⊗	TEAMS01	sip.pstnhub.microsoft.com	52.114.7.24:5061	✓	OPTIONS	available
⊗	TEAMS02	sip2.pstnhub.microsoft.com	52.114.132.46:5061	✓	OPTIONS	available
⊗	TEAMS03	sip3.pstnhub.microsoft.com	52.114.76.76:5061	✓	OPTIONS	available

Click submit to commit the configuration at the end of the page.

Add Actions:

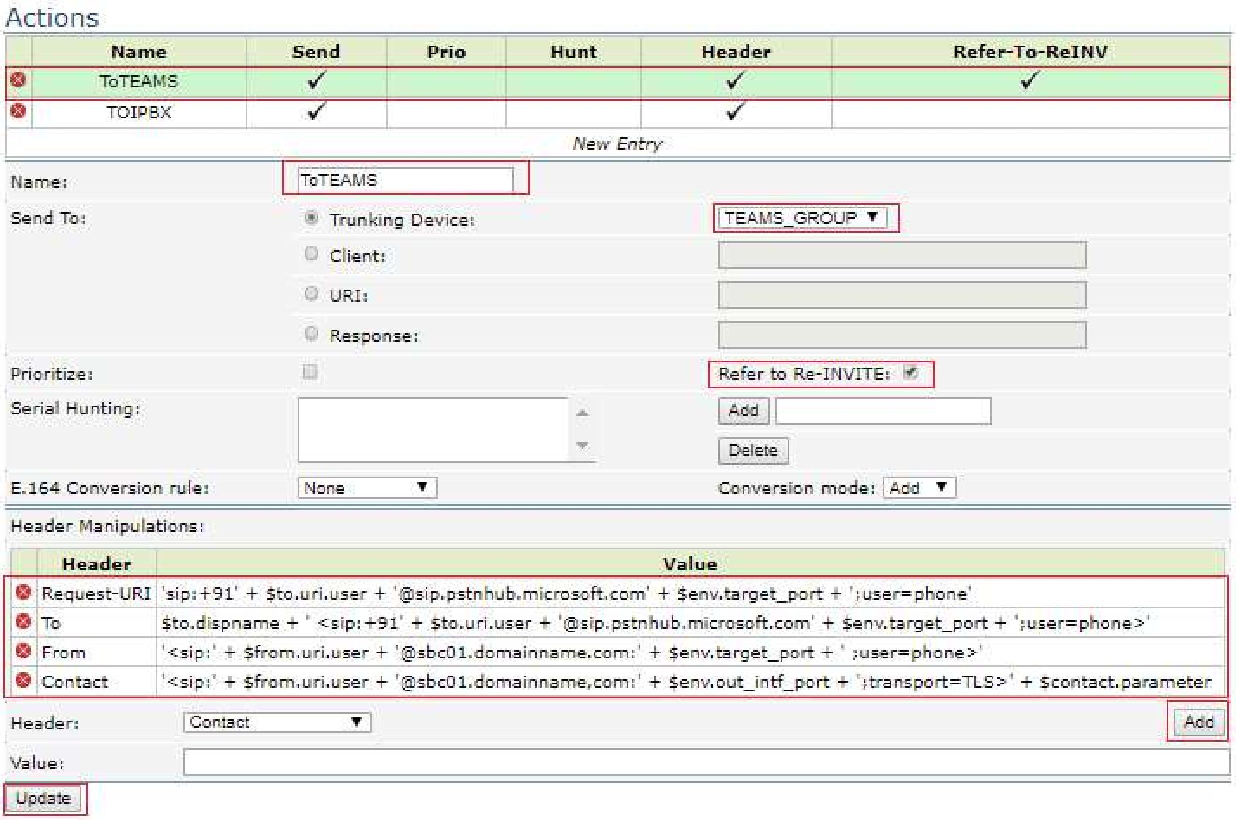
To Teams:

Add HMR rules as per the tenant FQDN.

The HMR rules can be customized as per the needs and country code during the *implementation*

HMR Rules towards Teams:

Request-URI	'sip:+91' + $to.uri.user + '@sip.pstnhub.microsoft.com' + $env.target_port + ';user=phone'
To	$to.dispname + ' <sip:+91' + $to.uri.user + '@sip.pstnhub.microsoft.com' + $env.target_port + ';user=phone>'
From	'<sip:' + $from.uri.user + '@sbc01.domainname.com:' + $env.target_port + ' ;user=phone>'
Contact	'<sip:' + $from.uri.user + '@sbc01.domainname.com:' + $env.out_intf_port + ';transport=TLS>' + $contact.parameter



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
☒	ToTEAMS	✓			✓	✓
☒	TOIPBX	✓			✓	

New Entry

Name: ToTEAMS

Send To: ● Trunking Device: TEAMS_GROUP ▼
○ Client:
○ URI:
○ Response:

Prioritize: □ Refer to Re-INVITE: ☑

Serial Hunting:

E.164 Conversion rule: None ▼ Conversion mode: Add ▼

Header Manipulations:

	Header	Value
☒	Request-URI	'sip:+91' + $to.uri.user + '@sip.pstnhub.microsoft.com' + $env.target_port + ';user=phone'
☒	To	$to.dispname + ' <sip:+91' + $to.uri.user + '@sip.pstnhub.microsoft.com' + $env.target_port + ';user=phone>'
☒	From	'<sip:' + $from.uri.user + '@sbc01.domainname.com:' + $env.target_port + ' ;user=phone>'
☒	Contact	'<sip:' + $from.uri.user + '@sbc01.domainname,com:' + $env.out_intf_port + ';transport=TLS>' + $contact.parameter

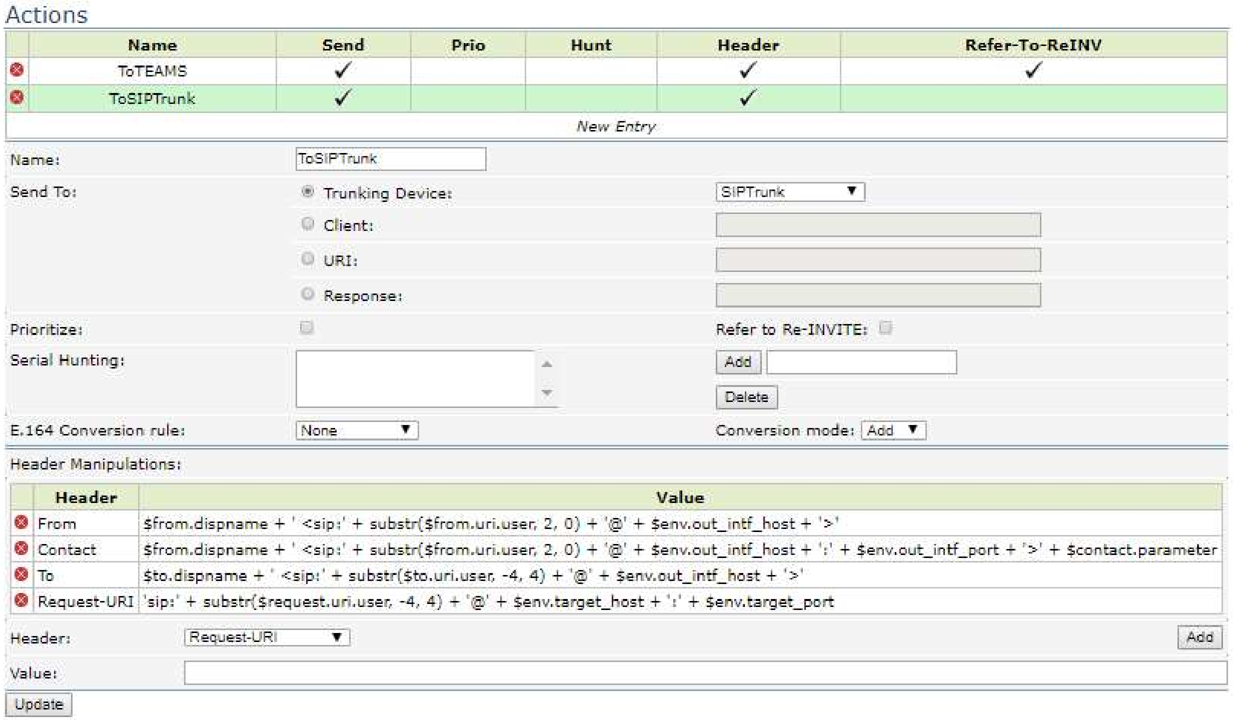
Header: Contact ▼

Value:

ToSIPServer:

Add HMR rules if requested to manipulate the values towards SIP-Trunk

The HMR rules can be customized as per the needs and country code during the implementation



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
⊗	ToTEAMS	✓			✓	✓
⊗	ToSIPTrunk	✓			✓	

New Entry

Name: ToSIPTrunk

Send To: ● Trunking Device: SIPTrunk ▼
○ Client:
○ URI:
○ Response:

Prioritize: □ Refer to Re-INVITE: □

Serial Hunting: Add Delete

E.164 Conversion rule: None ▼ Conversion mode: Add ▼

Header Manipulations:

	Header	Value
⊗	From	$from.dispname + ' <sip:' + substr($from.uri.user, 2, 0) + '@' + $env.out_intf_host + '>'
⊗	Contact	$from.dispname + ' <sip:' + substr($from.uri.user, 2, 0) + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>' + $contact.parameter
⊗	To	$to.dispname + ' <sip:' + substr($to.uri.user, -4, 4) + '@' + $env.out_intf_host + '>'
⊗	Request-URI	'sip:' + substr($request.uri.user, -4, 4) + '@' + $env.target_host + ':' + $env.target_port

Header: Request-URI ▼ Add

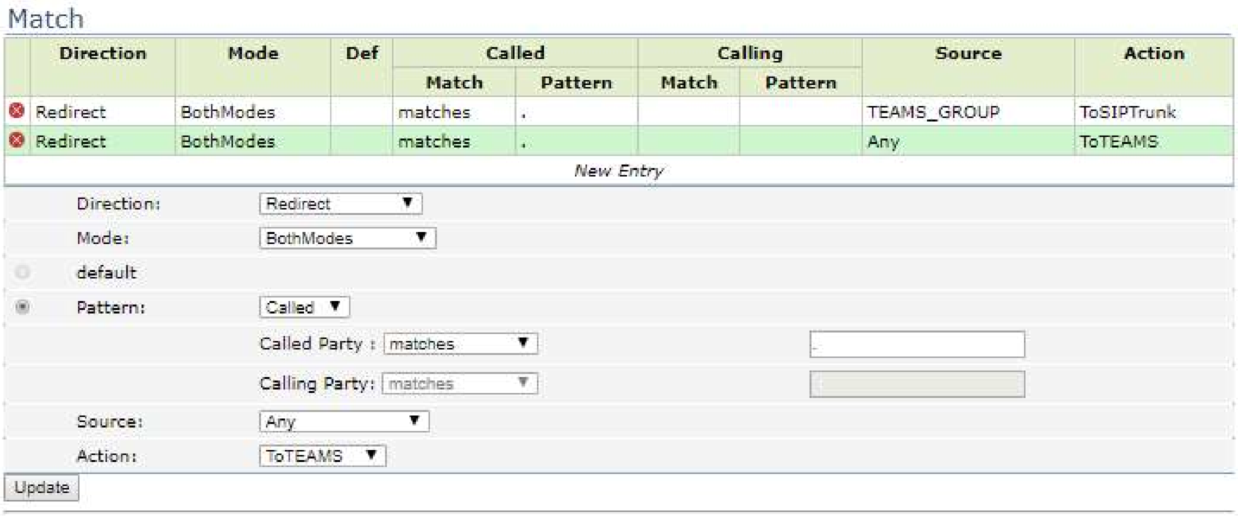
Value:

Update

Ribbon EdgeMarc Teams-DR Configuration

Add Route Match

ToTEAMS



Match

	Direction	Mode	Def	Called		Calling		Source	Action
				Match	Pattern	Match	Pattern		
✖	Redirect	BothModes		matches	.			TEAMS_GROUP	ToSIPTrunk
✖	Redirect	BothModes		matches	.			Any	ToTEAMS

New Entry

Direction: Redirect ▼

Mode: BothModes ▼

○ default

● Pattern: Called ▼

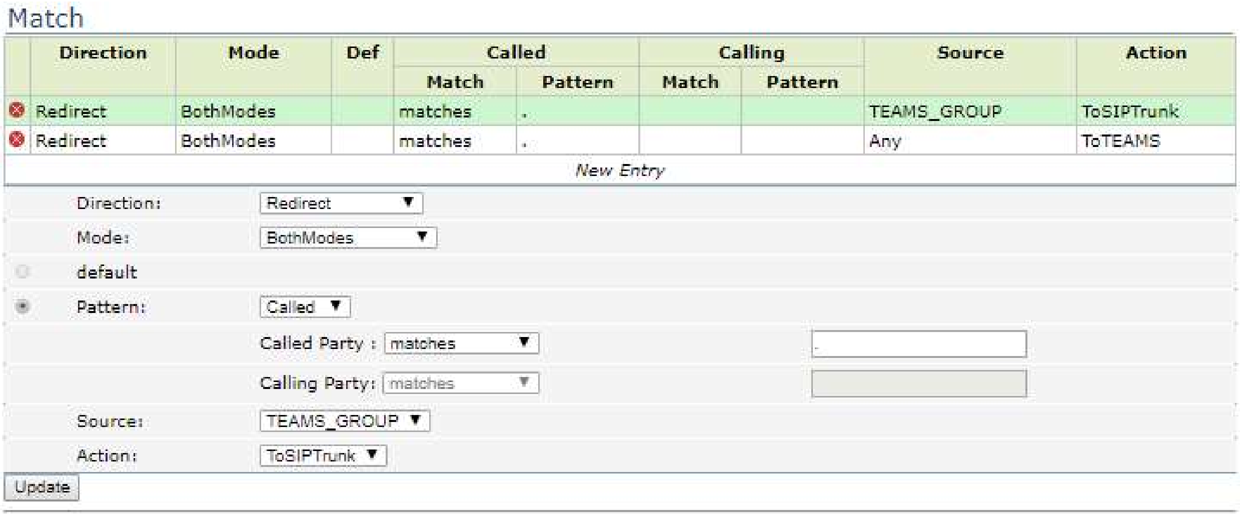
Called Party : matches ▼ .

Calling Party: matches ▼

Source: Any ▼

Action: ToTEAMS ▼

ToSIPTrunk:



Match

	Direction	Mode	Def	Called		Calling		Source	Action
				Match	Pattern	Match	Pattern		
✖	Redirect	BothModes		matches	.			TEAMS_GROUP	ToSIPTrunk
✖	Redirect	BothModes		matches	.			Any	ToTEAMS

New Entry

Direction: Redirect ▼

Mode: BothModes ▼

○ default

● Pattern: Called ▼

Called Party : matches ▼ .

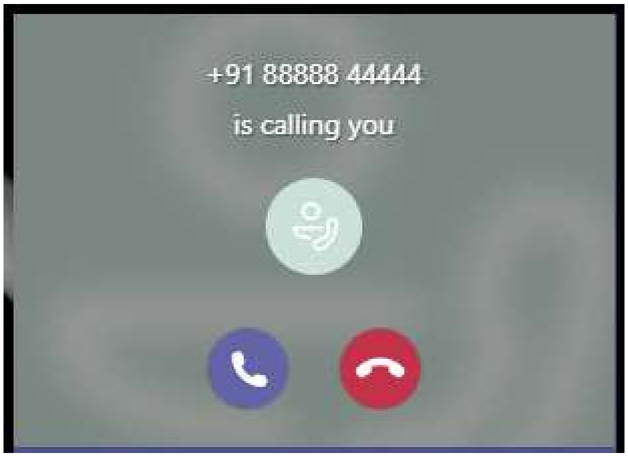
Calling Party: matches ▼

Source: TEAMS_GROUP ▼

Action: ToSIPTrunk ▼

Make Teams Call

Now Make a call from SIP Trunk to Teams and vice versa



+91 88888 44444

is calling you

Appendix:

Certificate Types:

Option 1 - Single SBC:

A certificate with a single SBC FQDN.

The SBC FQDN must be in the subject, common name and the Subject Alternate name.

SN/CN	SAN
{Public FQDN of SBC }	{Public FQDN of SBC }

Option 2 - Multiple SBC:

A certificate with a multiple SBC FQDN's.

The SBC FQDN must be in the subject, common name and the Subject Alternate name, which includes the additional SBCs too.

SN/CN	SAN
{Public FQDN of SBC }	{Public FQDN of SBC }, {Public FQDN of Additional SBC }, {Public FQDN of Additional SBC }

Option 3 – Single/ Multiple SBCs with wildcard:

A Wildcard certificate with a any FQDN in the common name and Subject Alternative Name (SAN), including the wildcard and SBC FQDN

SN/CN	SAN
{Public FQDN of SBC }	{ wildcard }, {Public FQDN of SBC }

How to generate CSR using Openssl:

Create a config for CSR generation with SAN (only when same cert needs to be used for multiple FQDN)

cat SAN.cnf

change the values of DNS.1 and DNS.2 as per your need (Paste the below contents to file named SAN.cnf)

```
[ req ]
default_bits       = 2048
distinguished_name = req_distinguished_name
req_extensions     = req_ext
attributes         = req_attributes
output_password    = mypass
[ req_distinguished_name ]
countryName                = Country Name (2 letter code)
stateOrProvinceName        = State or Province Name (full name)
localityName               = Locality Name (eg, city)
organizationName           = Organization Name (eg, company)
commonName                 = Common Name (e.g. server FQDN or YOUR name)
emailAddress                                   = Enter your organization email Address
OU                                                                  = Organization Unit Name (eg, Business Unit)
[ req_attributes ]
challengePassword          = A challenge password
[ req_ext ]
subjectAltName = @alt_names
[alt_names]
DNS.1   = sg.rbbn.com
DNS.2   = *.sg.rbbn.com
```

```
openssl req -out D:\BIN\TEAMS_CERT.csr -newkey rsa:2048 -nodes -keyout D:\BIN\private.key -config D:\BIN\SAN.cnf
```

Save the private key (will be used during the cert import into SBC)

Verify the CSR and get the signed cert by CA, input the generated CSR information.

https://www.sslshopper.com/csr-decoder.html

once get the signed cert, convert the cert to pfx (if required) using below command

```
openssl pkcs12 -export -out D:\BIN\TEAMS_CERT.pfx -inkey D:\BIN\private.key -in D:\BIN\TEAMS_CERT.crt
```

Ribbon EdgeMarc Teams-DR Configuration

Setting up PSTN Gateway on MS Teams

Set up PowerShell as per below link

https://docs.microsoft.com/en-us/microsoftteams/teams-powershell-overview

Example of configuring PSTN gateway using PowerShell

```
$credential = Get-Credential "prakash@domainname.com”

$SfBSession = New-CsOnlineSession -Credential $credential

Import-PSSession $SfbSession


New-CsOnlinePSTNGateway -Fqdn sbc01.domainname.com -SipSignallingPort 5061 -Enabled $true

Set-CsUser -Identity "prakash@domainname.com" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true -
OnPremLineURI tel:+9199999555555

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

New-CsOnlineVoiceRoute -Identity "To_EdgeMARC" -NumberPattern "^\+91(\d{10})$" -OnlinePstnGatewayList
sbc01.domainname.com -OnlinePstnUsages To_EdgeMARC

New-CsOnlineVoiceRoutingPolicy "Voice_Route_EdgeMARC" -OnlinePstnUsages "To_EdgeMARC"

Grant-CsOnlineVoiceRoutingPolicy -Identity "prakash@domainname.com" -PolicyName "Voice_Route_EdgeMARC"

Grant-CsTeamsCallingPolicy -PolicyName Allowcalling -Identity "prakash@domainname.com"
```