Ribbon EdgeMarc SBC Configuration with Microsoft Teams

Table of Contents

Document Overview

This document outlines the configuration best practices for the Ribbon EdgeMarc SBC when deployed with Microsoft Teams (Bring Your Own Carrier).

A Session Border Controller (SBC) is a network element deployed to protect SIP based Voice over Internet Protocol (VoIP) networks. Early deployments of SBCs were focused on the borders between two service provider networks in a peering environment. This role has now expanded to include significant deployments between a service provider's access network and a backbone network to provide service to residential and/or enterprise customers. The interoperability compliance testing focuses on verifying inbound and outbound calls flows between Ribbbon EdgeMarc and Microsoft Teams cloud. The Ribbon EdgeMarc SBC is deployed on the customer site to resolve any potential numbering format issues between Zoom and the customer's existing carrier dial plan numbering.

The Microsoft Teams solution can include other services that your installation may support to provide services beyond adding the Ribbon SBC for voice SBC support.

The Ribbon SBC is a configured service to the overall Microsoft Teams solution, the SBC normalizes MS-Teams based voice protocols to any SIP voice Trunking provider for PSTN access.

Microsoft Teams is deployed in the cloud on the WAN network and services multiple applications for the users. Remote or mobile are supported through MS-Teams cloud instance and can be configured to use the Ribbon SBC as their PSTN voice gateway.

The enterprise has chosen voice SIP Trunking support as IP-to-IP service for PSTN access.

Ribbon's SBC will provide the intercommunication support from MS-Teams to the SIP Trunking provider for PSTN access and security for the solution.

SIP UDP/RTP will be used for the SIP Trunking provider. SIP TLS/SRTP will be used on the WAN network from MS-Teams.

This guide contains the following sections:

- Section A: EdgeMarc Configuration
    - Configuring the SBC WAN and LAN IP Addresses
    - Create a CSR
    - Configuring the SBC VOIP Settings
    - Configuring the B2BUA and Header Manipulation Rules
    - Save the ESBC Configuration
- Section B: Microsoft Teams Configuration
    - Configuring Microsoft Teams
    - Obtain IP address and FQDN
    - Domain Name
    - Obtain a Certificate
    - Public Certificate
    - Configure and Generate Certificates on the SBC
    - Configure Office 365 Tenant Voice Routing

References
For additional information on Zoom, refer to https://docs.microsoft.com/en-us/microsoftteams/.

For additional information on the Ribbon SBC, refer to https://ribboncommunications.com/.

Non-Goals

It is not the goal of this guide to provide detailed configurations that will meet the requirements of every customer. Use this guide as a starting point and build the SBC configurations in consultation with network design and deployment engineers.

Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring both the Ribbon SBCs and the third-party product. Steps will require navigating the third-party product as well as the Ribbon SBC Command Line Interface (CLI). Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP is needed to complete the configuration and any necessary troubleshooting.

Note
This configuration guide is offered as a convenience to Ribbon customers. The specifications and information regarding the product in this guide are subject to change without notice. All statements, information, and recommendations in this guide are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided “AS IS”. Users must take full responsibility for the application of the specifications and information in this guide.

Product and Device Details

The sample configuration in this document uses the following equipment and software:

Table 1: Requirements

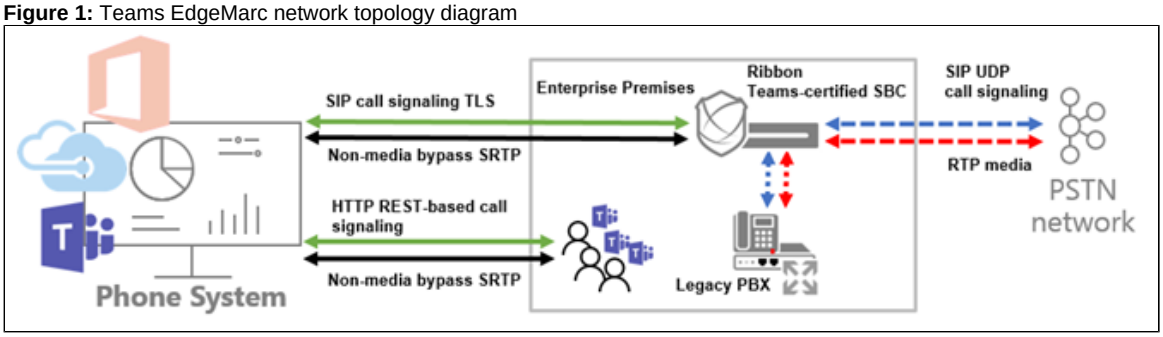
	Equipment	Software Version
Ribbon Communications	Ribbon EdgeMarc	V15.6.1
Microsoft Teams		

> **Note**
> Configuration guide is designed keeping EdgeMarc as a representative model with the software version V15.6.1 but it applies to all models in the EdgeMarc portfolio (300, 2900, 480x, 6000, 7301, 7400) with the same software version.

Network Topology Diagram

The following topology diagram shows connectivity between Microsoft Teams and Ribbon EdgeMarc.

Figure 1: Teams EdgeMarc network topology diagram



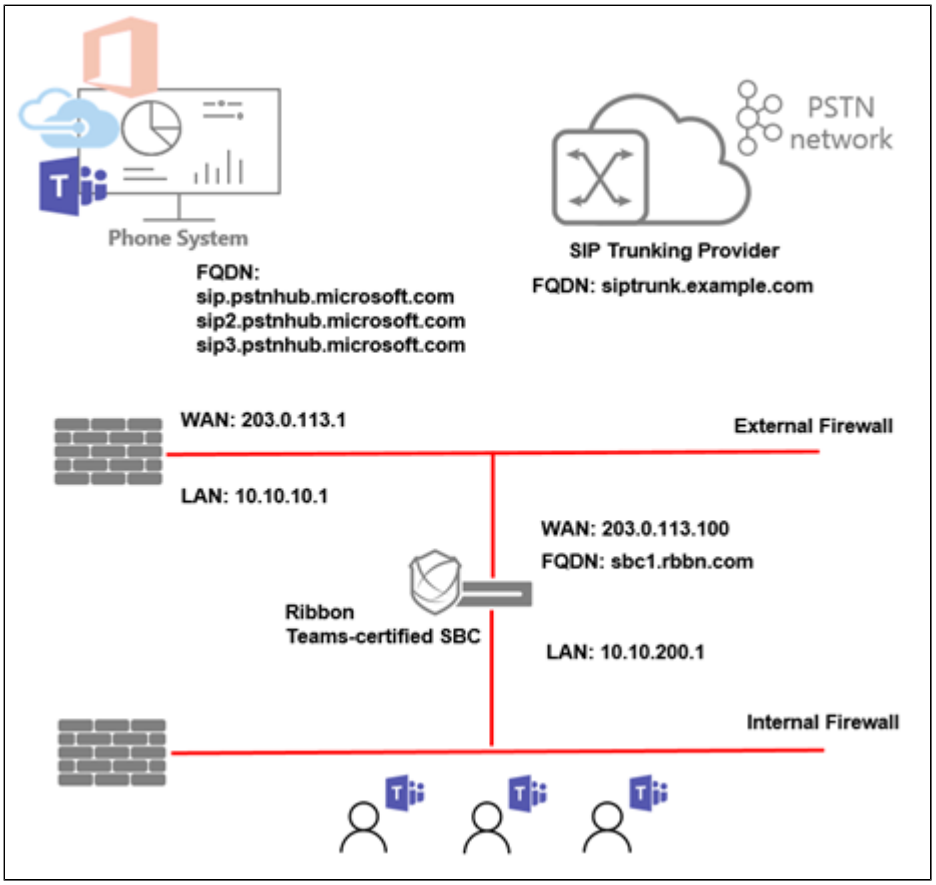
Section A: EdgeMarc Configuration

The following EdgeMarc configurations are included in this section:

1. Configuring the SBC WAN and LAN IP Addresses
2. Create a CSR
3. Configuring the SBC VOIP Settings
4. Configuring the B2BUA and Header Manipulation Rules
5. Save the ESBC Configuration

There are multiple network methods to deploying the Ribbon SBC MS-Teams SIP Trunking support. The SBC's WAN interface can be configured with a public IP directly to the perimeter security device and firewall filter rules for the ports required applied to the firewall policy or placed directly on the public network. The SBC's WAN interface is protected by its own firewall and dynamically assigns RTP/SRTP ports for the duration of the SIP session from an array of configurable ports. The SBC is configured in a private DMZ deployment with a public IPv4 address provided by the perimeter security device. In this model, the perimeter security device must not provide NAT or PAT to the public IPv4 address forwarded to the SBC. This will be the model chosen for the SBC's configuration discussed in the document.

Figure 2: ESBC Public WAN IP deployment



Configuring the SBC WAN and LAN IP Addresses

1. The system default LAN IP is 192.168.1.1 with username: root and password: default.
Attach LAN Port 1 of the system to the LAN network or directly to the management computer for the first-time IP networking setup.

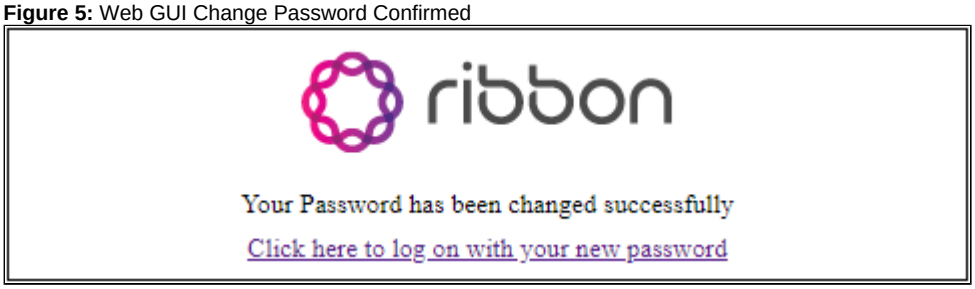
Figure 3: First Time GUI Login to the SBC

2. The system will prompt you to change the default password.

Figure 4: Web GUI Change Password

3. After the password change is confirmed, click the link to login with the new password.

Figure 5: Web GUI Change Password Confirmed



4. The landing page will appear. From the left-hand navigation menu select **Network**.

Figure 6: Web GUI Landing Page

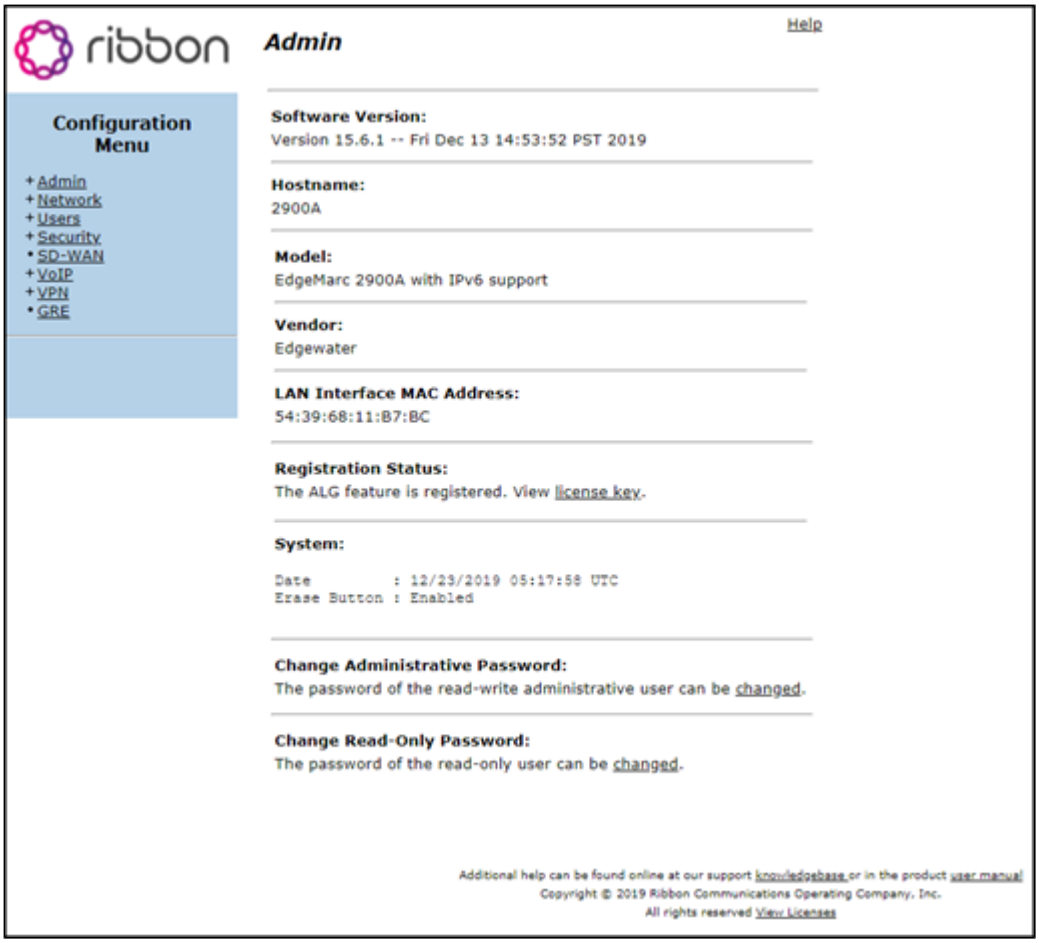
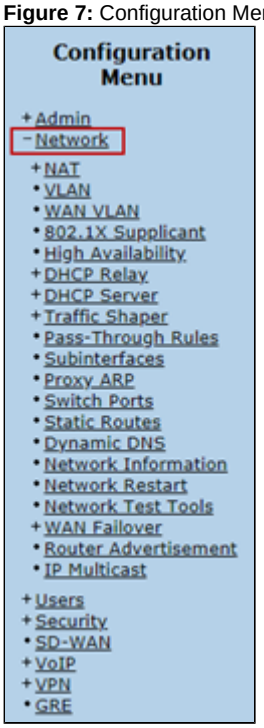
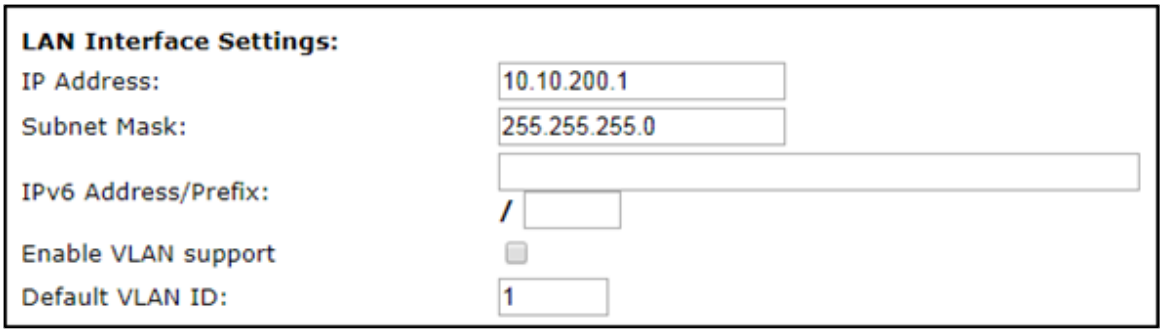


Figure 7: Configuration Menu Network



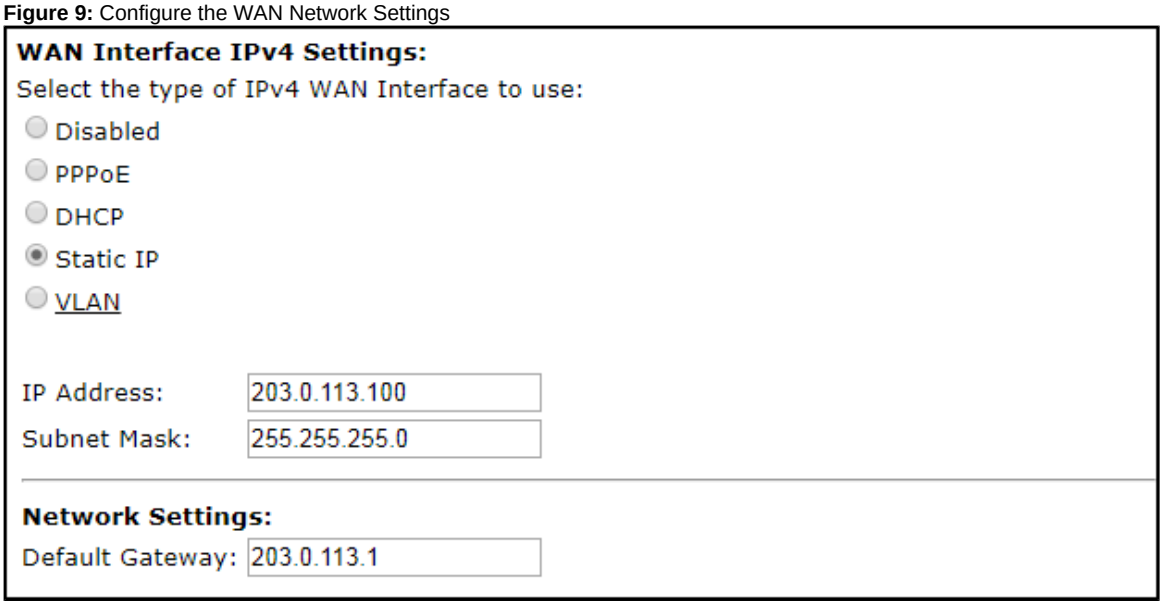
5. Configure the LAN Interface settings.

Figure 8: Configure the LAN Network Settings



6. Configure the WAN Interface and Default Gateway Settings.

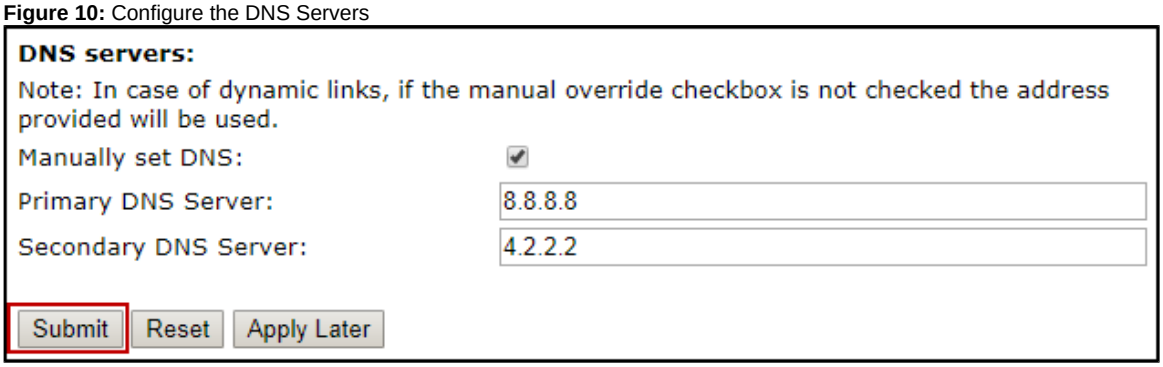
Figure 9: Configure the WAN Network Settings



7. Configure the Primary and the Secondary DNS to a public DNS server and select **Submit**. The system will now apply the networks settings.

8. Install the system on the network and reconnect from the management computer to the configured LAN IPv4 Address, and login.

Figure 10: Configure the DNS Servers



Create a CSR

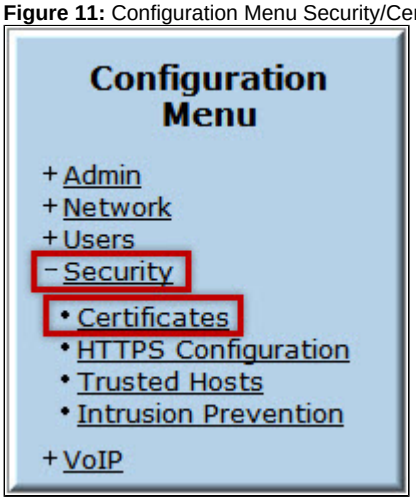
Generate a Certificate Signing Request and obtain the certificate from a supported Certification Authority (CA).

This step discusses how to create a certificate signing request (CSR) to be signed by an approved Microsoft documentation certificate authority. The certificate is used by the SBC for TLS SIP signaling support to MS-Teams. This signed certificate will be applied to the WAN interface of the system.

Many CA's do not support a private key with a length of 1024 bits. Validate with your CA requirements and select the appropriate length of the key.

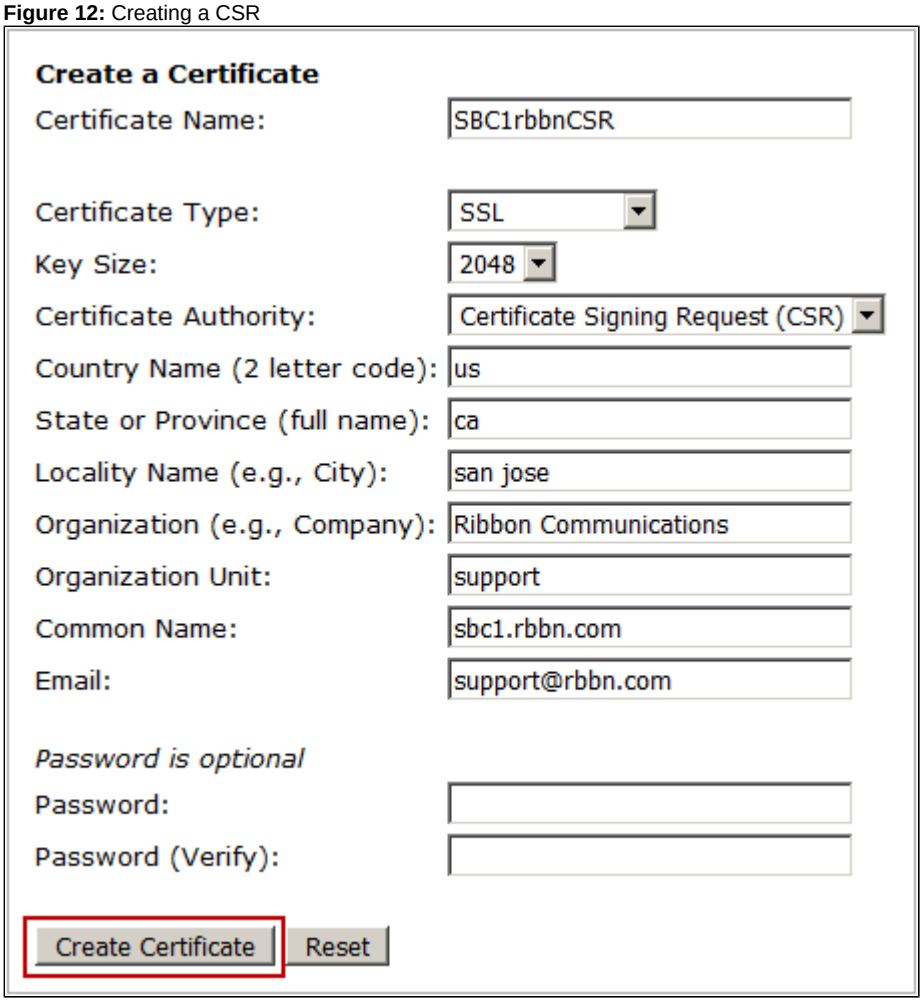
1. From the left-hand navigation menu select **Security** > **Certificates**.

Figure 11: Configuration Menu Security/Certificates



2. Using the Create a Certificate pane, enter the data for the fields as it applies to your system.

Figure 12: Creating a CSR



Create the CSR as follows:

Parameter	Example Configuration Value

Certificate Name:	Arbitrary name (alpha/numeric characters only)
Certificate Type:	SSL
Key Size:	2048
Certificate Authority:	Certificate Signing Request (CSR)
Country Name (2 letter code):	Us
State or Province (full name):	Ca
Locality Name (e.g., City):	San Jose
Organization (e.g., Company):	Ribbon Communications
Organization Unit:	support
Common Name:	sbc1.rbbn.com (This name must be identical to the name configured as the PSTN gateway - New-CsOnlinePSTNGateway) value
Email:	support@rbbn.com
Password:	*Password is optional and should not be set for MS-Teams*
Password (Verify):	*Password is optional and should not be set for MS-teams*

3. Click to download the CSR certificate and key file and save to the management computer.

Figure 13: Download the CSR

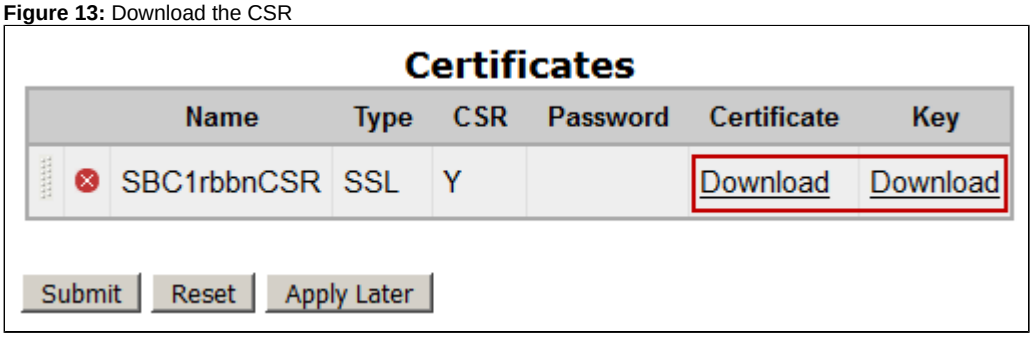
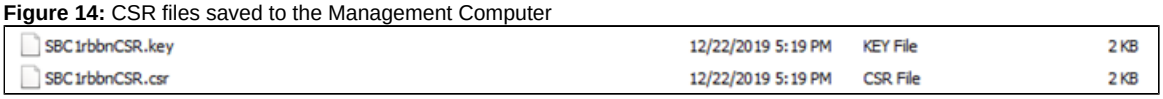


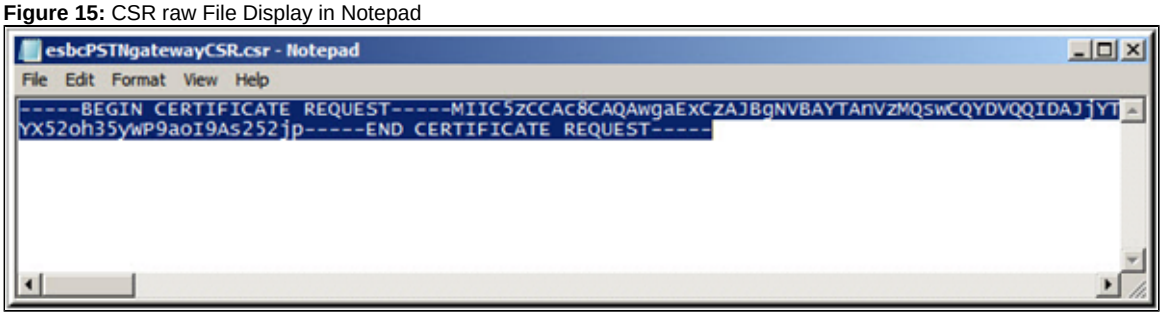
Figure 14: CSR files saved to the Management Computer



4. Open the .csr file with an application such as Notepad and copy the complete certificate request:

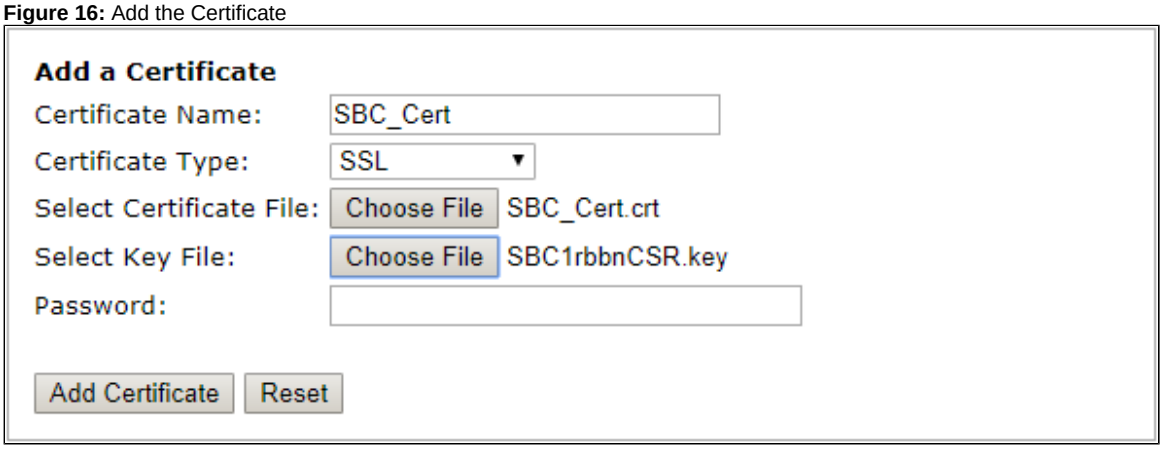
-----BEGIN CERTIFICATE REQUEST-----
MIIC5zCCAc8CAQAwgaExCzAJBgNVBAYTAnVzMQswCQYDVQQIDAJjYTERMA8GA1UEBwwIc2FuIGpvc2UxGzAZBgNVBAoMEkVkZ2V3YXRlciBOZXR3b3JrczEQMA4GA1UECwwHc3VwcG9ydDEVMBMGA1UEAwwMZXNiYy5ld25pLnVzMSwwKgYJKoZIhvcNAQkBFh1zdXBwb3J0QGVkZ2V3YXRlcm5ldHdvcmtzLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANXHkMUH
/MHmMyJksO0BwP5T34nA60JlgrTGoqXKrGlqKv55WGh29QFiXa90v7a
/qqnsNFMOK+tKhz6v4+tylLtEZrjPEyY8PhH4DDVYj5iFp+YKB+YLg6KFv9c1TtIeD1i9RsosyPQxKFJMq4JZhAjKYQXQSXFn89pKCrBEK0VFNJrAkqq
5OtxvAYmiEWl4h9DtnU6syDcCJDRI9ogNNfwiSz3xjHZ46OsyFch4gpFA0oBq06CRC43sRxrSOL3G4ZKutg
/Nd1JJ7pGoXm7Y3FbvZEgPuXrH5uTiM8vRHAetRmiLZDP4ivkwzbWTHv+X9njcjs8oO6Dy0gYJ2shAGO0CAwEAAaAAMA0GCSqGSIb3DQEBCwUA
A4IBAQDMn9N4EOWRBtkQzAI6l7yYun96IhG+UbOhCKwM/XD4J+7iDTKQ12q09ZKj0KvEqqOyPMFe8LbeQpLcKTGppjUsKS/L9sZ9
/QvVt34uFV0Qcts1IZP+pOq0ZsMD7dHaVlZLEq4ohDh8I3UFZkyDGLGxeM
/ir8jEnJSUKUGb21pFNcT1sJI+YelNwhy0m7+osnPO40cP+fgs4dchQ5OAaGa97OHxHI/5DC1b
/3trHOq32jJJGALAYtl7kprMDayd0cbqG1hj342HQSeSuUOx5a4OEf4J5U0sw0pvGWyE7amkttTBHUmFB9dnvYGLM80CZYX52oh35yWP9aoI9As252
jp-----END CERTIFICATE REQUEST-----

Figure 15: CSR raw File Display in Notepad



5. Configure the signed certificate on the system in the **Add a Certificate** pane on the Certificates page. Click **Add Certificate**. The signed certificate must use the .key file from the CSR generation.

Figure 16: Add the Certificate

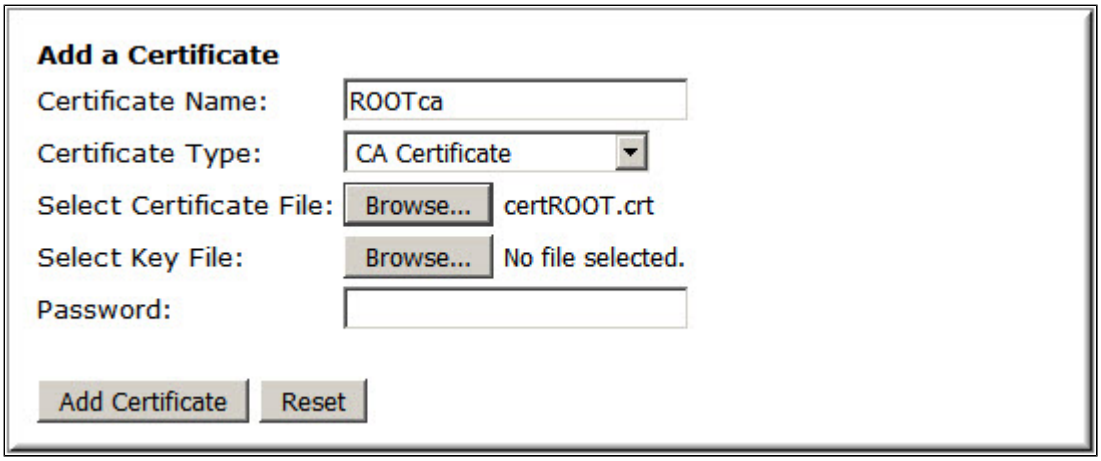


Configure the Certificate as follows:

Parameter	Example Configuration Value
Certificate Name:	SBC_Cert Arbitrary name (alpha/numeric characters only)
Certificate Type:	SSL
Select Certificate File:	SBC_Cert.crt
Select Key File:	SBC1rbbnCSR.key
Password:	*Password is optional and should not be set for Skype for Business*

6. Download the root CA on the system and click **Add Certificate**.

Figure 17: Add the root CA



Configure the Root CA as follows:

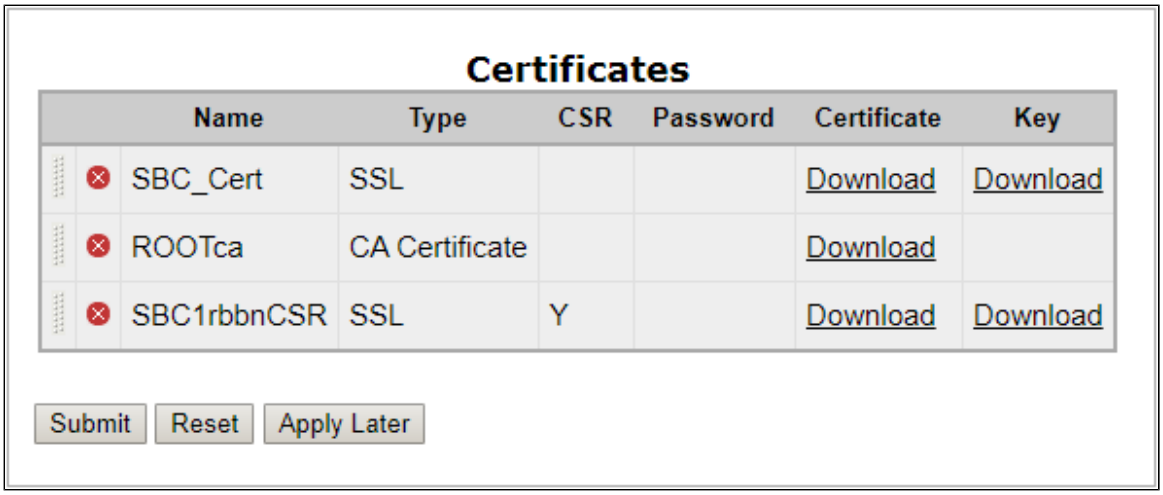
Parameter	Example Configuration Value
Certificate Name:	ROOTca Arbitrary name (alpha/numeric characters only)
Certificate Type:	CA Certificate
Select Certificate File:	certROOT.crt
Select Key File:	No File Selected (No key file is required for a root CA)
Password:	*Password is optional and should not be set for Skype for Business*

7. Select **Submit All** to save the certificates to the system.

Figure 18: Submit All Certificate to the ESBC

The certificates are now displayed and available to be assigned to system services.

Figure 19: Certificates are Displayed



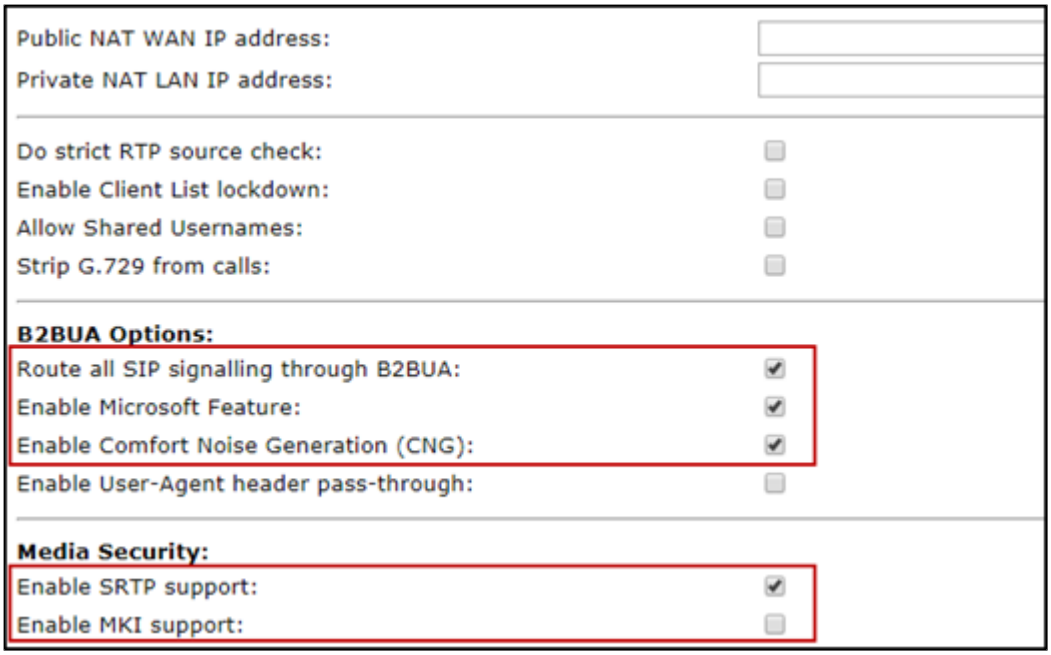
Configuring the SBC VOIP Settings

1. From the left-hand navigation menu select **VoIP**.

Figure 20: Configuration Menu VoIP

2. Configure the system's VoIP settings.

Figure 21: Configure VoIP parameters



Configure VoIP parameters as follows:

Parameter	Example Configuration Value
Enable LLDP:	Enabled (default)
LLDP Broadcast Interval (sec):	30 (default)
TFTP Server IP address:	Disabled
Use ALG Alias IP Addresses:	Disabled
Public NAT WAN IP address:	Public WAN IPv4 address when using a 1-to-1 NAT configuration
Private NAT LAN IP address:	Private LAN IPv4 address when using a 1-to-1 NAT configuration
Do strict RTP source check:	Disabled
Enable Client List lockdown:	Disabled
Allow Shared Usernames:	Disabled
Strip G.729 from calls:	Disabled
Route all SIP signalling through B2BUA:	Enabled
Enable Microsoft Feature:	Enabled
Enable Comfort Noise Generation (CNG):	Enabled
Enable User-Agent header pass-through:	Disabled
Enable SRTP support:	Enabled
Enable MKI support:	Disabled - (Optional, this depends on if MKI support is enabled on MS-Teams)
H.225/H.245 Port Range:	14085-15084 (default)

RTP Port Range:	16386-18385 (default)
RTP Packetization Time (ms):	20
Prioritize Microsoft Teams:	Not Required for MS-Team, the system will automatically prioritize signaling and media. This setting is used when the system is “NATing” MS-Teams traffic
Calculate RTT:	Enabled (default)

3. Configure the SIP Server settings for the SIP Trunking service parameters.

Figure 22: Configure SIP parameters

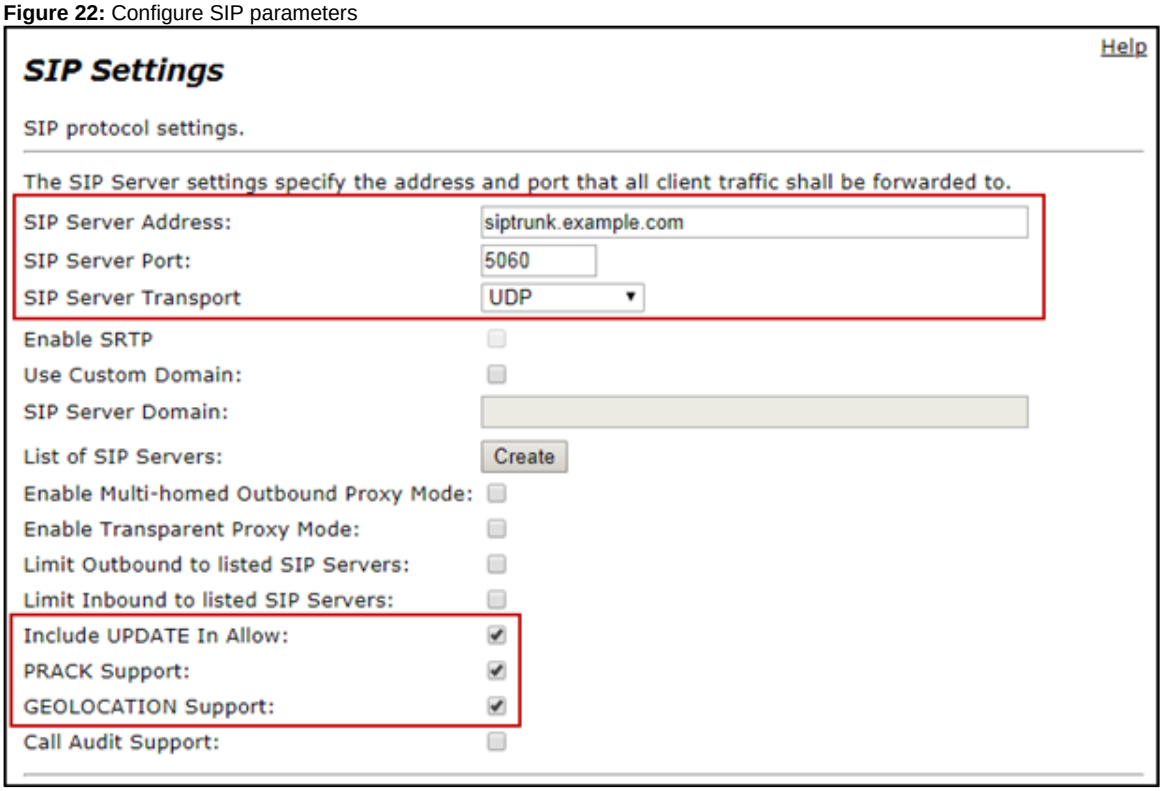


Figure 23: Configure SIP parameters

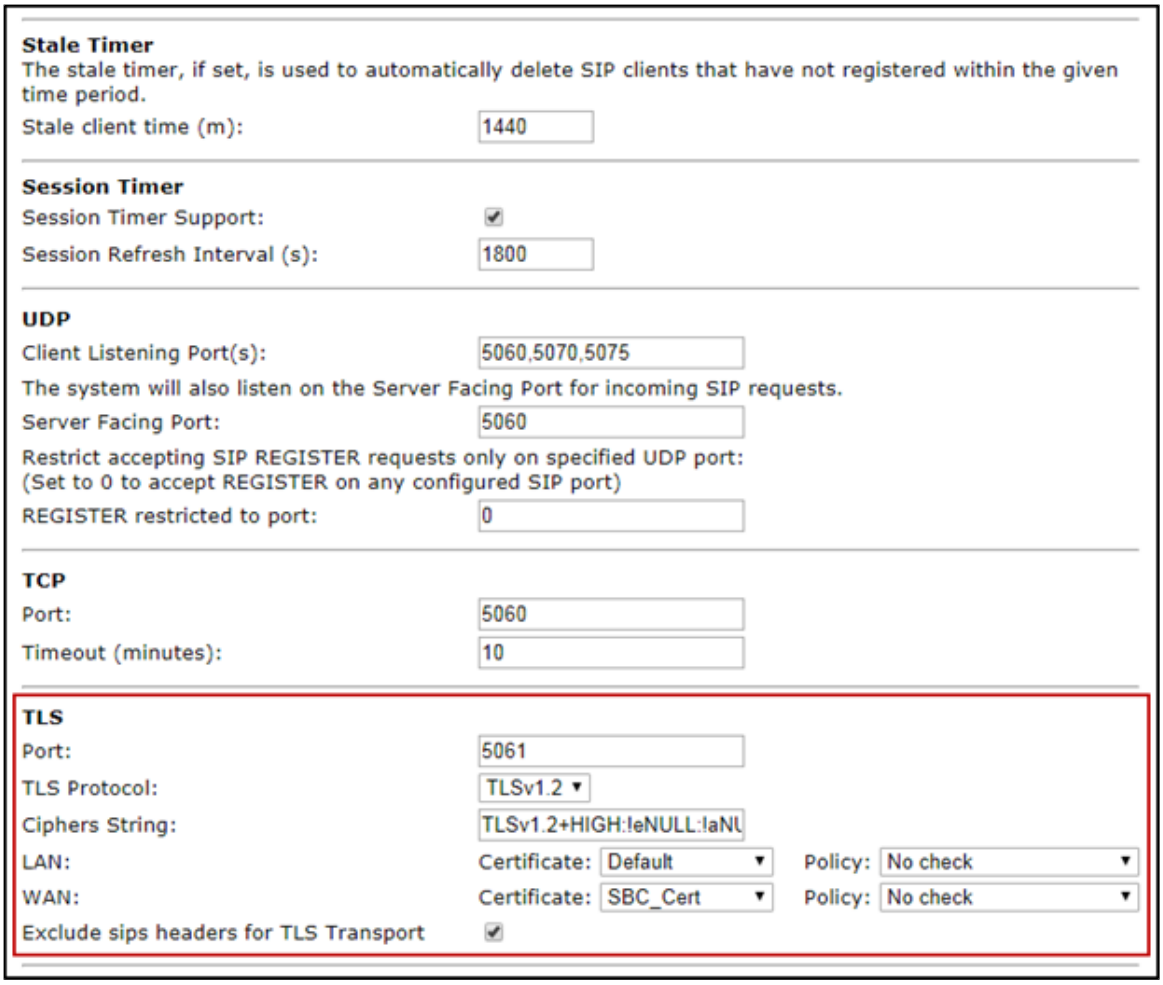
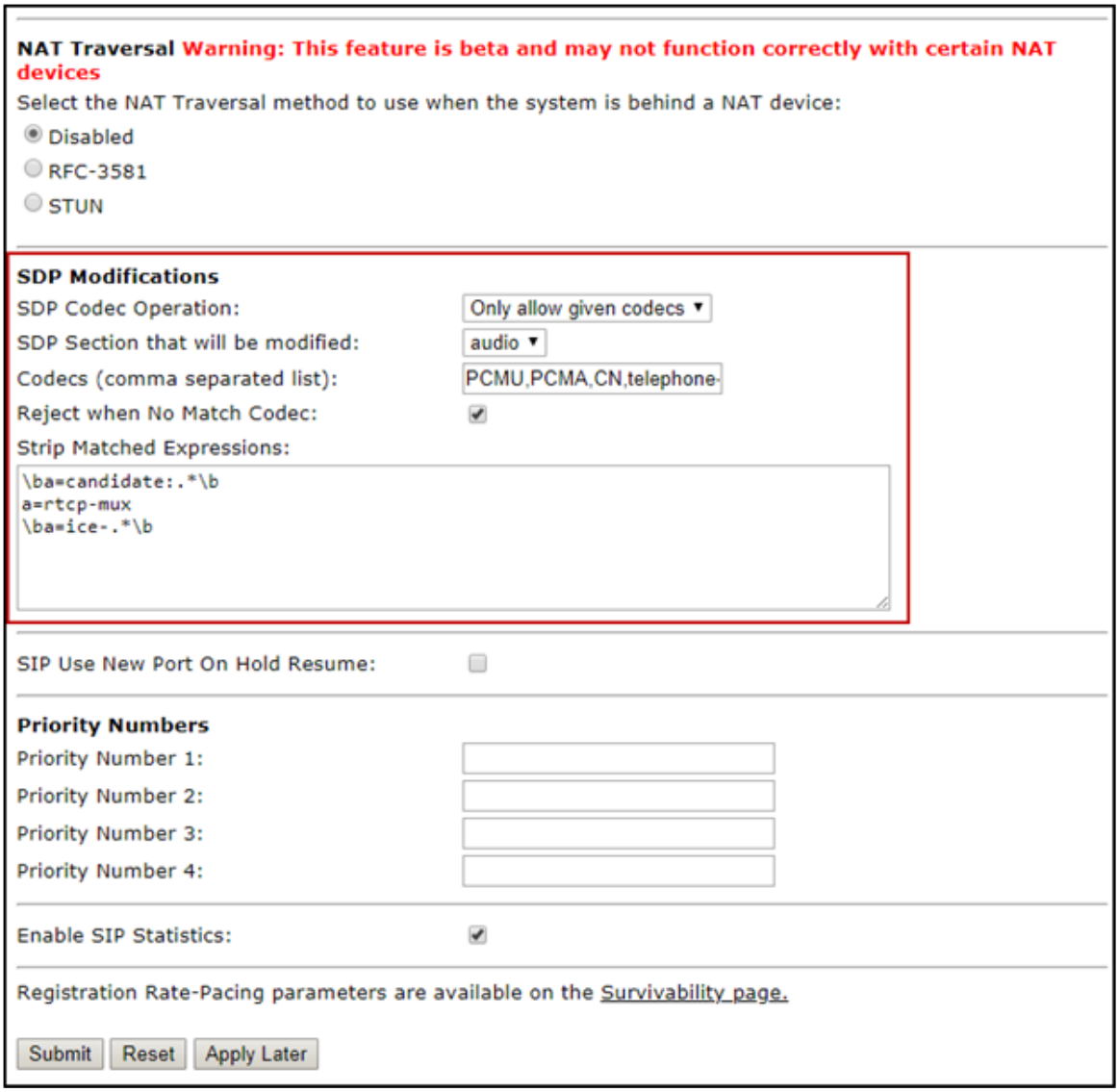


Figure 24: Configure SIP parameters



Configure SIP Server Settings as follows:

Parameter	Example Configuration Value
SIP Server Address	siptrunk.example.com
SIP Server Port	5060 (Verify with your SIP trunking provider which SIP port to configure) **Note**: If the FQDN resolves to a different port for the SIP Server Address the system will use the port returned in the DNS query response.
SIP Server Transport	UDP
Enable SRTP	Disabled
Use Custom Domain:	Disabled
SIP Server Domain:	Not set
List of SIP Servers:	none
Enable Multi-homed Outbound Proxy Mode:	Disabled
Enable Transparent Proxy Mode:	Disabled
Limit Outbound to listed SIP Servers:	Disabled

Limit Inbound to listed SIP Servers:		Disabled	
Include UPDATE In Allow:		Enabled	
PRACK Support:		Enabled	
GEOLOCATION Support:		Enabled	
Call Audit Support:		Disabled	
Stale client time (m):		1440 (default)	
Session Timer Support:		Enabled	
Session Refresh Interval (s):		1800 (default)	
UDP	**Client Listening Port(s):**	5060,5070,5075 (default)	
UDP	**Server Facing Port:**	5060 (default)	
UDP	**REGISTER restricted to port:**	0 (default)	
TCP	**Port:**	5060 (default)	
TCP	**Timeout (minutes):**	10 (default)	
TLS	**Port:**	5061	
TLS	**TLS Protocol:**	TLSv1.2	
TLS	**Ciphers String:**	TLSv1.2+HIGH:!eNULL:!aNULL	
TLS	**LAN:**	Certificate: Default	Policy: No Check
TLS	**WAN:**	Certificate: SBC_Cert	Policy: No Check
TLS	**Exclude sips headers for TLS Transport**	Enabled	
NAT Traversal		Disabled RFC-3581 STUN	
SDP Codec Operation:		Allow only given codecs	
SDP Section that will be modified:		audio	
Codecs (comma separated list):		PCMU,PCMA,CN,telephone-event	
Reject when No Match Codec:		Enabled	
Strip Matched Expressions:		\ba=candidate:.*\b a=rtcp-mux \ba=ice-.*\b	
SIP Use New Port On Hold Resume:		Disabled	
Priority Number 1: **Priority Number 2:** **Priority Number 3:** **Priority Number 4:**		Not set	
Enable SIP Statistics:		Enabled	

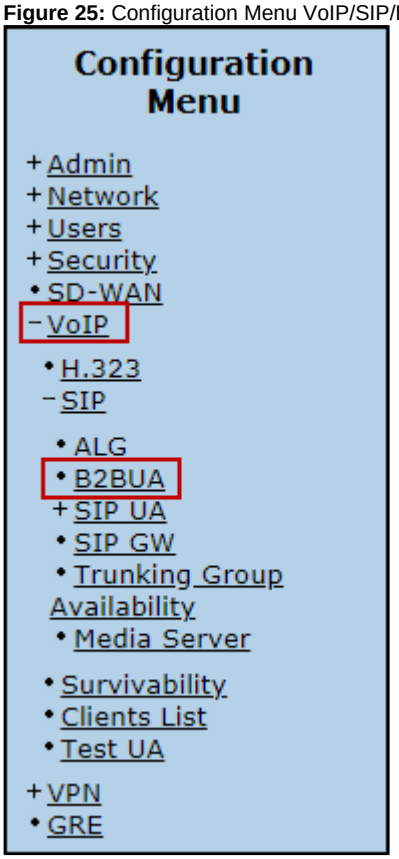
4. Click **Submit** to apply the changes.

Configuring the B2BUA and Header Manipulation Rules

This step discusses how to configure a B2BUA Trunking device to the WAN side of the system for MS-Teams support. Header manipulation rules will be used to modify the headers required for interoperability to/from MS-Teams and to/from the SIP Trunking provider.

1. From the left-hand navigation menu select **VoIP > SIP > B2BUA.**

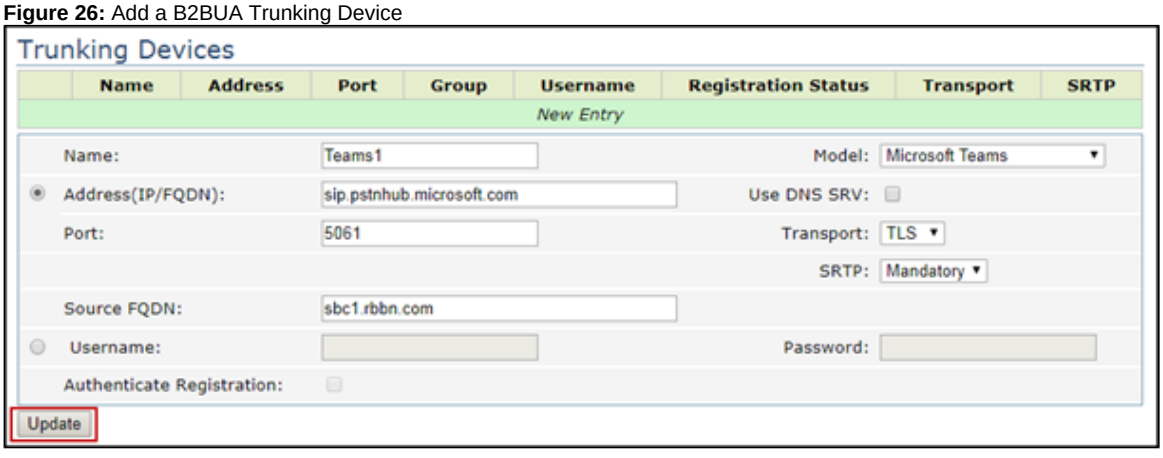
Figure 25: Configuration Menu VoIP/SIP/B2BUA



2. Add a B2BUA Trunking Device for the MS-Teams cloud servers and click **Update**.

3. Scroll to the bottom and click **Submit**.

Figure 26: Add a B2BUA Trunking Device

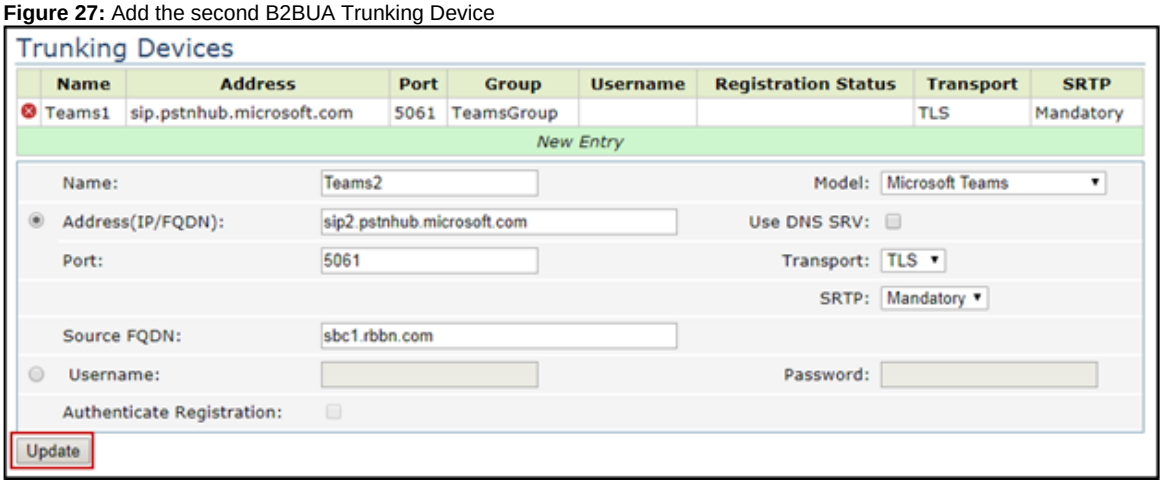


Configure the B2BUA Trunk as follows:

Parameter	Example Configuration Value

Name:	Teams1 Arbitrary name (alpha/numeric characters only)
Model:	Microsoft Teams
Address(IP/FQDN):	sip.pstnhub.microsoft.com
Use DNS SRV:	Not set for MS-Teams
Port:	5061
Transport:	TLS
SRTP:	Mandatory
Source FQDN:	sbc1.rbbn.com (This name must be identical to the name configured as the PSTN gateway)
Username:/Password:	Not used for MS-Teams

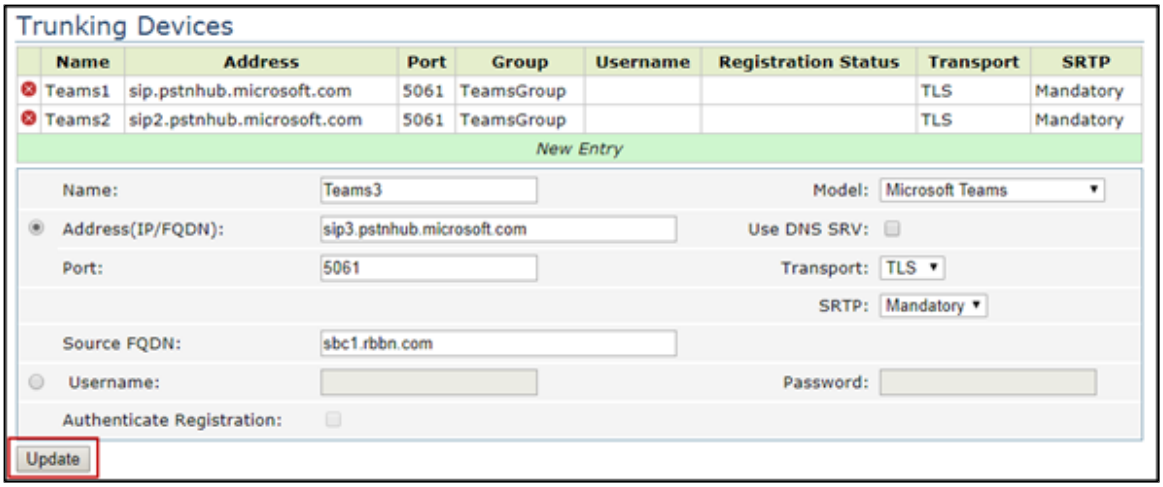
Figure 27: Add the second B2BUA Trunking Device



Configure the second B2BUA Trunk as follows:

Parameter	Example Configuration Value
Name:	Teams2 Arbitrary name (alpha/numeric characters only)
Model:	Microsoft Teams
Address(IP/FQDN):	sip2.pstnhub.microsoft.com
Use DNS SRV:	Not set for MS-Teams
Port:	5061
Transport:	TLS
SRTP:	Mandatory
Source FQDN:	sbc1.rbbn.com (This name must be identical to the name configured as the PSTN gateway)
Username:/Password:	Not used for MS-Teams

Figure 28: Add the third B2BUA Trunking Device



Configure the third B2BUA Trunk as follows:

Parameter	Example Configuration Value
Name:	Teams3 Arbitrary name (alpha/numeric characters only)
Model:	Microsoft Teams
Address(IP/FQDN):	sip3.pstnhub.microsoft.com
Use DNS SRV:	Not set for MS-Teams
Port:	5061
Transport:	TLS
SRTP:	Mandatory
Source FQDN:	sbc1.rbbn.com (This name must be identical to the name configured as the PSTN gateway)
Username:/Password:	Not used for MS-Teams

4. Create a routing group for the MS-Teams servers with the Trunking Group Availability function.

Figure 29: Configuration Menu VoIP/SIP/Trunking Group Availability

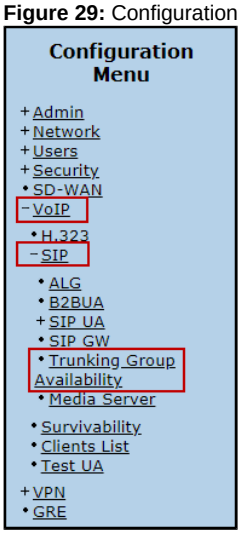


Figure 30: Create the Routing Group

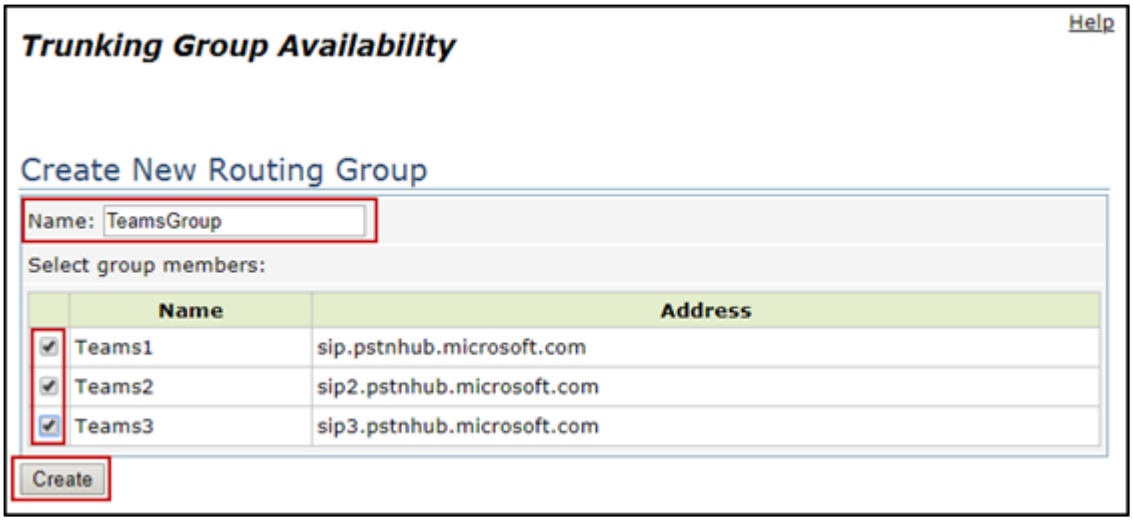
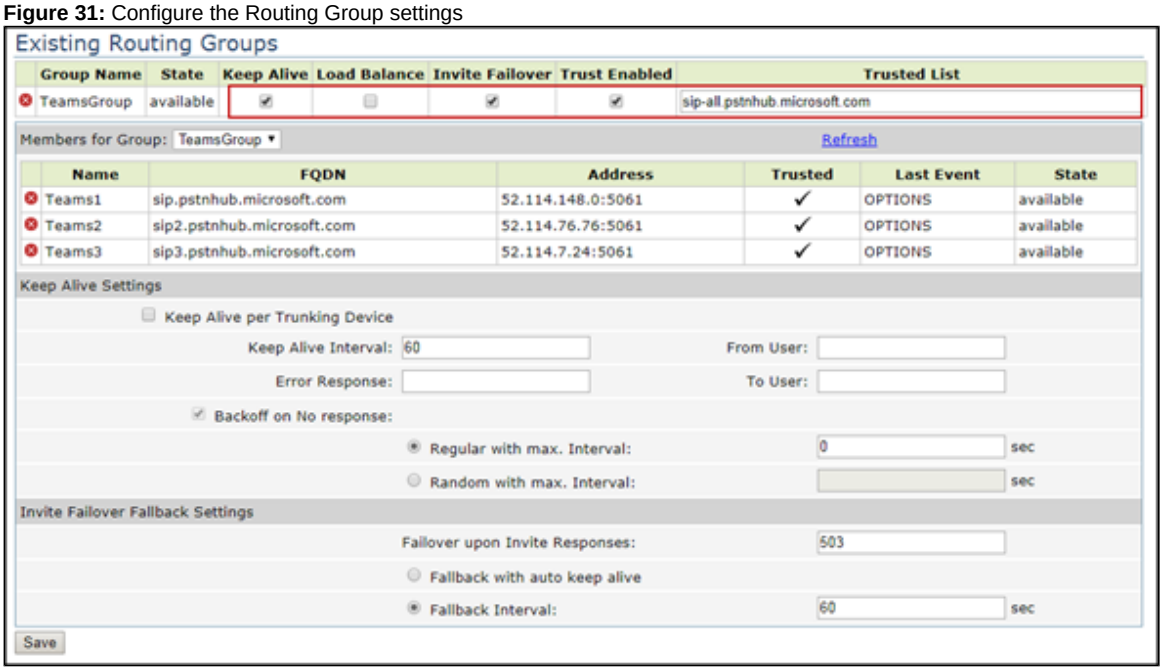


Figure 31: Configure the Routing Group settings



Configure the Routing Group as follows:

Parameter		Example Configuration Value
Group Name	**TeamsGroup**	N/A
State		Display Only
Keep Alive		Enabled
Load Balance		Optional
Invite Failover		Enabled
Trust Enabled		Enabled
Trusted List		sip-all.pstnhub.microsoft.com
Members for Group:		TeamsGroup
Keep Alive Interval:		60 (default)
Error Response:		Not Set

From User:		Not Set
To User:		Not Set
Backoff on No Response		Enabled
Regular with max. Interval:	Enabled	0sec (default)
Random with max. Interval:	N/A	N/A
Failover upon Invite Responses:		503
Fallback with auto keep alive		**Not Selected**
Fallback Interval:	**Enabled**	60(s) (default)

5. From the left-hand navigation menu select **VoIP > SIP > B2BUA**.
Header manipulation rules will be used to modify the headers required for interoperability to/from MS-Teams and to/from the SIP Trunking provider.

Figure 32: Configuration Menu VoIP/SIP/B2BUA

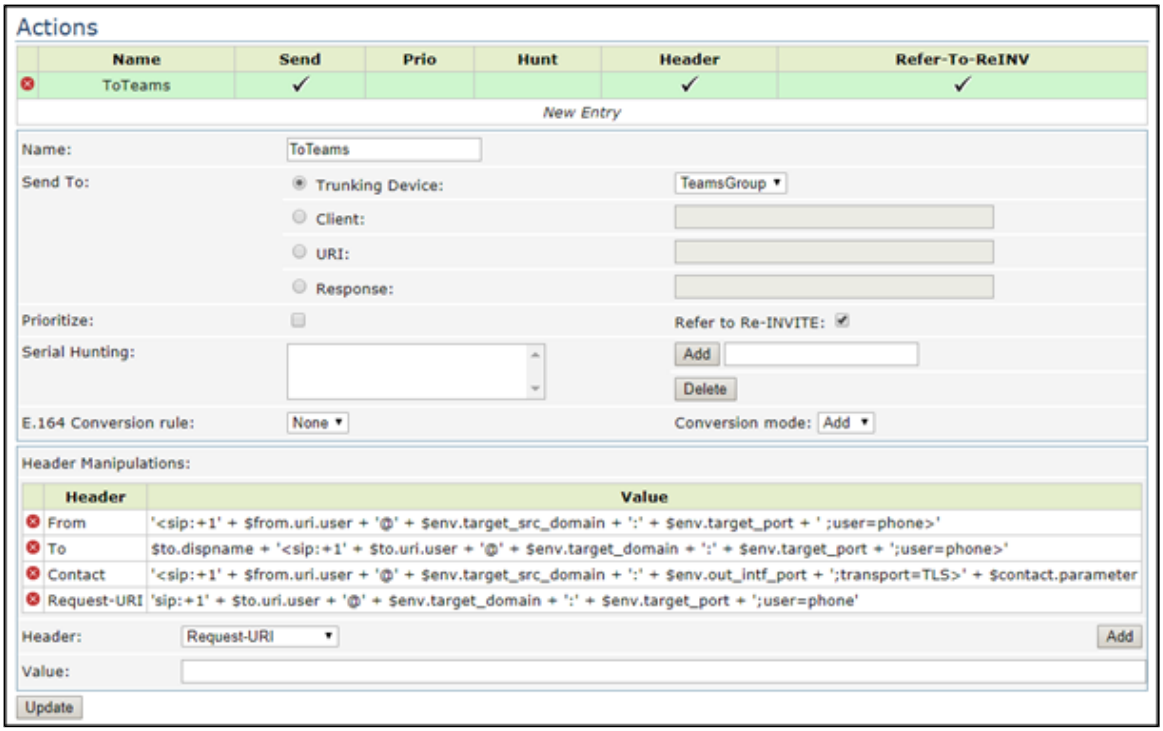
6. Scroll down to **Actions** and add the following actions and associated HMR rules. The first Actions is “ToTeams”. This rule will have an associated “Match” rule for calls going to Teams.

a) Configure the parameters in the actions pane.

b) Configure each Header Value one at a time and click Add before creating the next rule.

c) Click **Update** then Click **Submit** to save the Action.

Figure 33: Add Action ToTeams and HMR rules



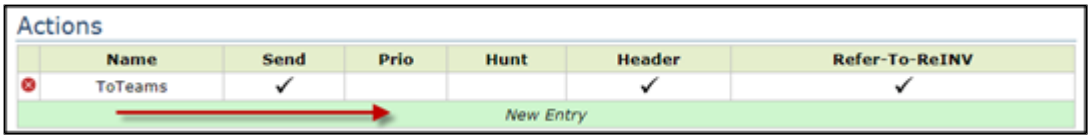
Configure the ToTeams Action as follows:

Parameter		Example Configuration Value
Name:		ToTeams Arbitrary name (alpha/numeric characters only)
Send To:	**Trunking Device:**	TeamsGroup
Prioritize:		Not used for MS-Teams
Refer to Re-INVITE:		Enabled
Serial Hunting:		Not used for MS-Teams
E.164 Conversion rule:		None
Conversion mode:		Add (default)
Header		Example Value
Request-URI		'sip:+1' + $to.uri.user + '@' + $env.target_domain + ':' + $env.target_port + ';user=phone'
From		'<sip:+1' + $from.uri.user + '@' + $env.target_src_domain + ':' + $env.target_port + ' ;user=phone>'
To		$to.dispname + '<sip:+1' + $to.uri.user + '@' + $env.target_domain + ':' + $env.target_port + ';user=phone>'
Contact		'<sip:+1' + $from.uri.user + '@' + $env.target_src_domain + ':' + $env.out_intf_port + ';transport=TLS>' + $contact.parameter

7. The second action is "FromTeams2ServerAnonymous", this rule will have an associated “Match” rule for calls with “Anonymous” in the SIP URI, for example, when a Teams caller is blocking their number the SIP From URI will have the following format From: "Anonymous"sip: anonymous@anonymous.invalid:5060. This rule allows anonymous calls inbound from Teams to the SIP Trunking provider.

To add a new Action click anywhere in the **New Entry** bar.

Figure 34: NewEntry

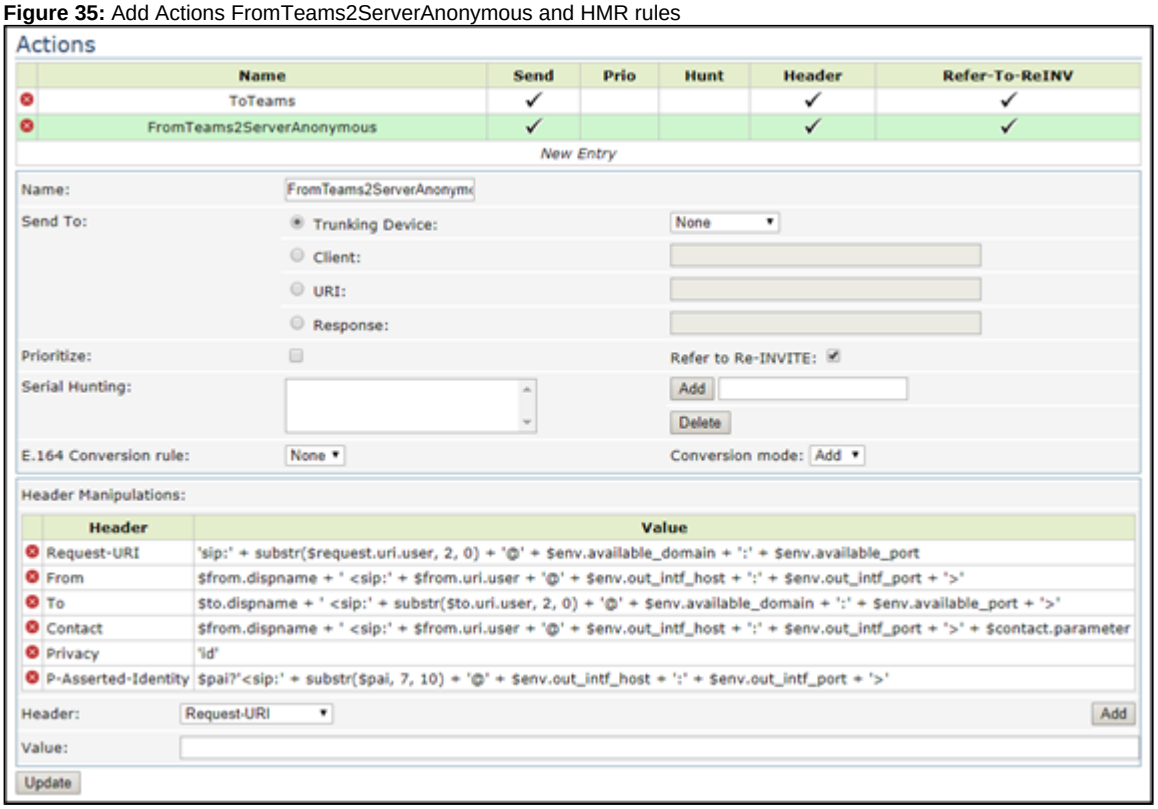


a) Configure the parameters in the actions pane.

b) Configure each Header Value one at a time and click **Add** before creating the next rule.

c) Click **Update** then Click **Submit** to save the Action.

Figure 35: Add Actions FromTeams2ServerAnonymous and HMR rules



Configure the FromTeams2ServerAnonymous Action as follows:

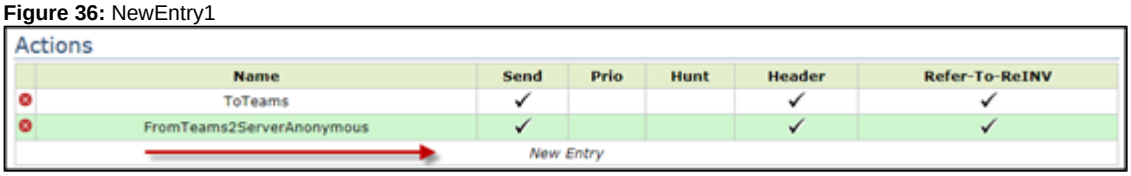
Parameter		Example Configuration Value
Name:		FromTeams2ServerAnonymous Arbitrary name (alpha/numeric characters only)
Send To:	**Trunking Device**	None
Prioritize:		Not used for MS-Teams
Refer to Re-INVITE:		Enabled
Serial Hunting:		Not used for Skype for Business
E.164 Conversion rule:		None
Conversion mode:		Add (default)
Header		Example Value
Request-URI		'sip:' + substr($request.uri.user, 2, 0) + '@' + $env.available_domain + ':' + $env.available_port
From		$from.dispname + ' <sip:' + $from.uri.user + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>'

To		$to.dispname + ' <sip:' + substr($to.uri.user, 2, 0) + '@' + $env.available_domain + ':' + $env.available_port + '>'
Contact		$from.dispname + ' <sip:' + $from.uri.user + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>' + $contact.parameter
P-Asserted-Identity		$pai?'<sip:' + substr($pai, 7, 10) + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>'
Other	**Privacy**	'id'

8. The third action is “FromTeams2Server”, this rule will have an associated “Match” rule for calls outbound from Teams to the SIP Trunking provider for destination call routing. This example uses a “P-Asserted-Identity” header string which is common to many SIP trunking providers, please verify with your trunking provider “if” they require these SIP headers or other header requirements to interoperate with their SIP service.

To add a new Action click anywhere in the **New Entry** bar.

Figure 36: NewEntry1

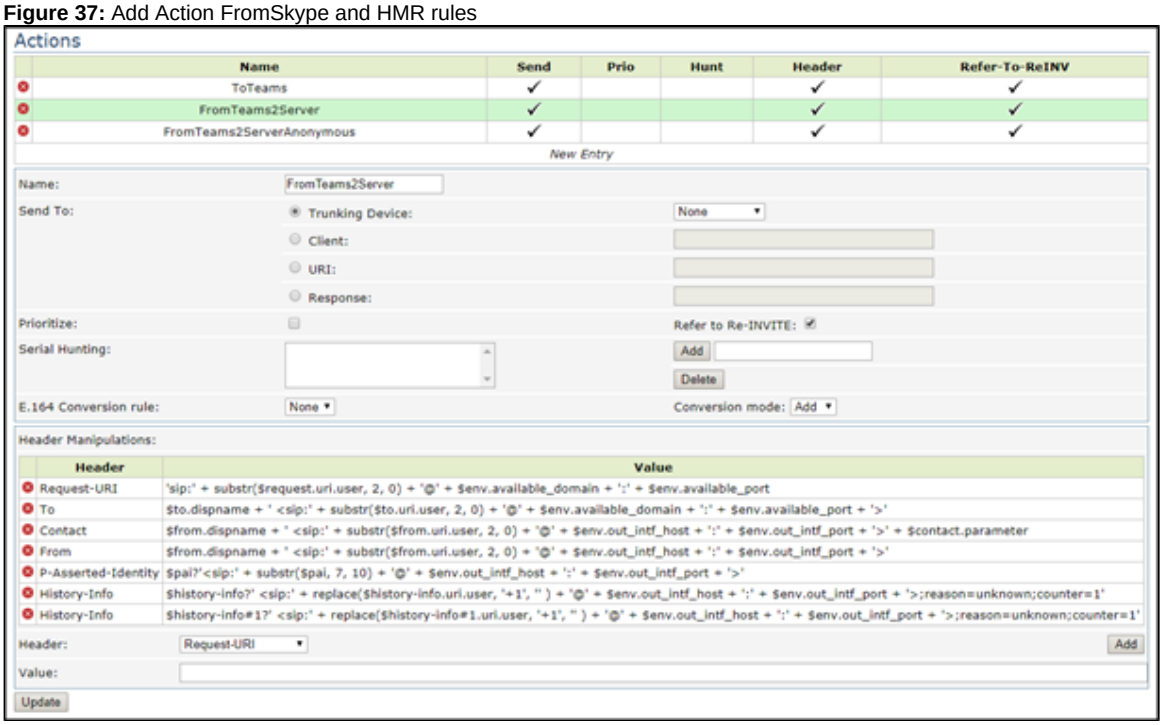


a) Configure the parameters in the actions pane.

b) Configure each Header Value one at a time and click **Add** before creating the next rule.

c) Click **Update** then Click **Submit** to save the Action.

Figure 37: Add Action FromSkype and HMR rules



Configure the FromTeams2Server Action as follows:

Parameter	Example Configuration Value

Name:		FromTeams2Server Arbitrary name (alpha/numeric characters only)
Send To:	**Trunking Device:**	None
Prioritize:		Not used for MS-Teams
Refer to Re-INVITE:		Enabled
Serial Hunting:		Not used for Skype for Business
E.164 Conversion rule:		None
Conversion mode:		Add (default)
Header		Example Value
Request-URI		'sip:' + substr($request.uri.user, 2, 0) + '@' + $env.available_domain + ':' + $env.available_port
From		$from.dispname + ' <sip:' + substr($from.uri.user, 2, 0) + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>'
To		$to.dispname + ' <sip:' + substr($to.uri.user, 2, 0) + '@' + $env.available_domain + ':' + $env.available_port + '>'
Contact		$from.dispname + ' <sip:' + substr($from.uri.user, 2, 0) + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>' + $contact.parameter
P-Asserted-Identity		$pai?'<sip:' + substr($pai, 7, 10) + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>'
History-info		$history-info?' <sip:' + replace($history-info.uri.user, '+1', '') + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>;reason=unknown;counter=1'
History-info		$history-info#1?' <sip:' + replace($history-info#1.uri.user, '+1', '') + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>;reason=unknown;counter=1'

9. Scroll down to the “Match” pane to configure the patterns you wish to match to the actions just created. The match function provides dial plan routing to Actions and relate to the direction the call is coming from, this could be from Teams or from the SIP trunking provider. The examples given in this section will use a dial plan of 408.555.1000-1099 to provide basic knowledge of how to apply your dial plan to the previously created Actions.

The example will use an “Redirect” rule from Teams as “+1.”, by default Teams will add this to the beginning of every outbound call going to the SBC for SIP trunk routing. This rule is mapped to the Action.”FromTeams2Server” which will remove the +1 from the SIP message and then perform the other header modifications before forwarding the SIP message to the trunking provider. If you’ve configured Teams to not add the +1 then modify the “FromTeams2Server” Action and other header manipulation rules that reference +1 and remove the reference.

The +1. (dot) portion of the string matches one or more digits this (dot) will allow dialed destinations greater than 10 or 11 digits to be called. If international calling is desired, verify the MS-Teams voice route to the SBC also includes pattern matches to accommodate international calling. 911, 411 and any other dial plans must also be considered as a SBC or MS-Teams pattern match to route the call correctly.

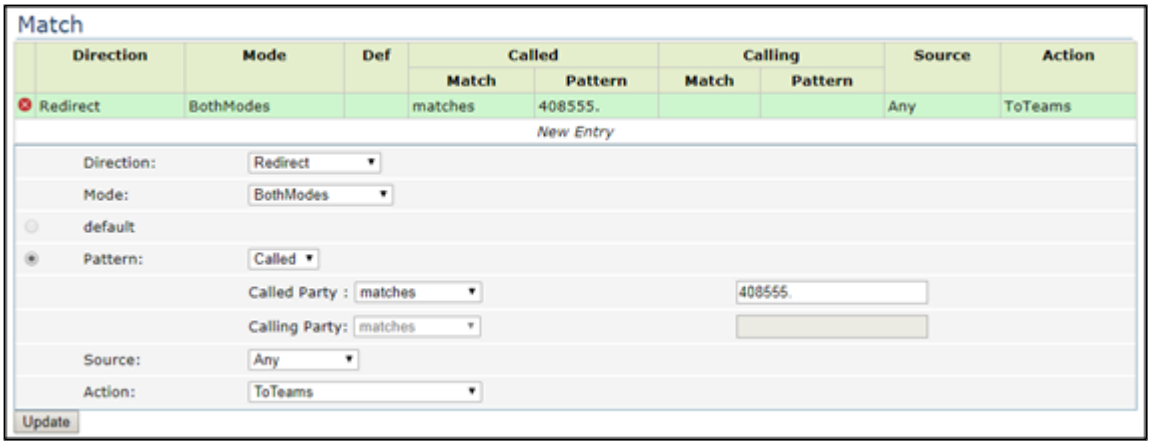
Note: Match rules are in order of priority from top to bottom, a specific rule must be above a generic rule.

10. The first “Match” rule will be for the Teams dial plan assigned by the SIP trunking provider in this example the DID range for this MS-Teams configuration is “408.555.1000-1099.

a) Configure the parameters in the match pane.

b) Click **Update** then Click **Submit** to save the Match.

Figure 38: Add Match - Called Matches ToTeams



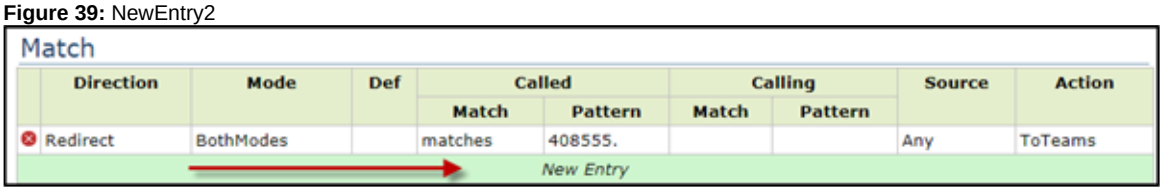
Configure the Called Matches ToTeams Match as follows:

Parameter		Example Configuration Value
Direction:		Redirect
Mode:		BothModes
Default:		Not used for MS-Teams
Pattern:		Called
Called Party:	**Matches**	408555.
Calling Party:	**Not Set**	N/A
Source:		Any
Action:		ToTeams

11. The second “Match” rule is to allow the blocked call-ID’s from Teams which presents as “anonymous” in the SIP header for example, From: "Anonymous"sip:anonymous@anonymous.invalid:5060.

a) To add a new Action click anywhere in the **New Entry** bar.

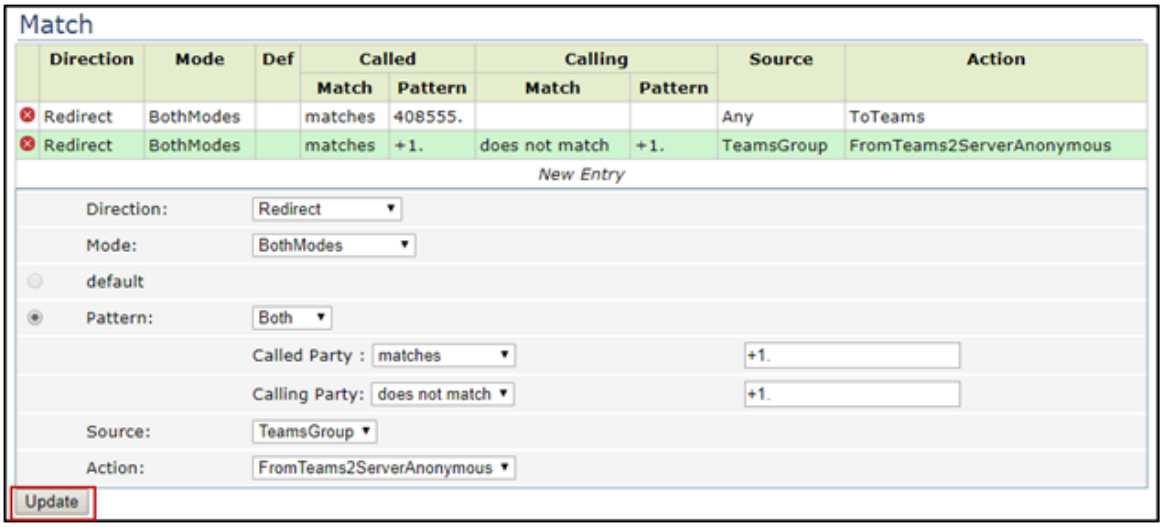
Figure 39: NewEntry2



b) Configure the parameters in the match pane.

c) Click **Update** then Click **Submit** to save the Match.

Figure 40: Add Match From Teams to Server Anonymous



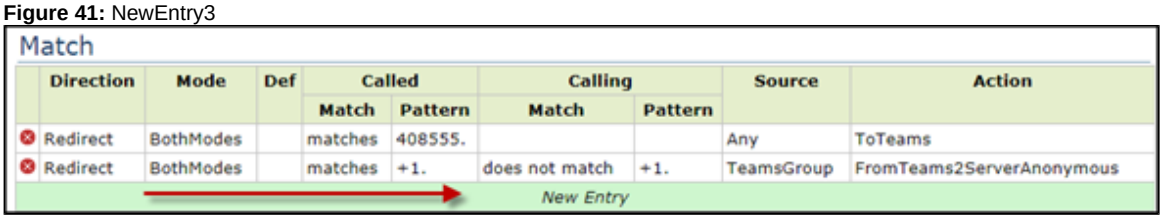
Configure the From Teams to Server Anonymous match as follows:

Parameter		Example Configuration value
Direction:		Redirect
Mode:		BothModes
Default:		Not used for MS-Teams
Pattern:		Both
Called Party:	**Matches**	+1.
Calling Party:	**Does not match**	+1.
Source:		TeamsGroup
Action:		FromTeams2ServerAnonymous

12. The third “Match” rule is to match +1. SIP messages from MS-Teams to the Actions that routes the call to the configured SIP trunking provider after the header manipulation has been performed. This rule is needed for normal caller-ID routing.

a) To add a new Action click anywhere in the **New Entry** bar.

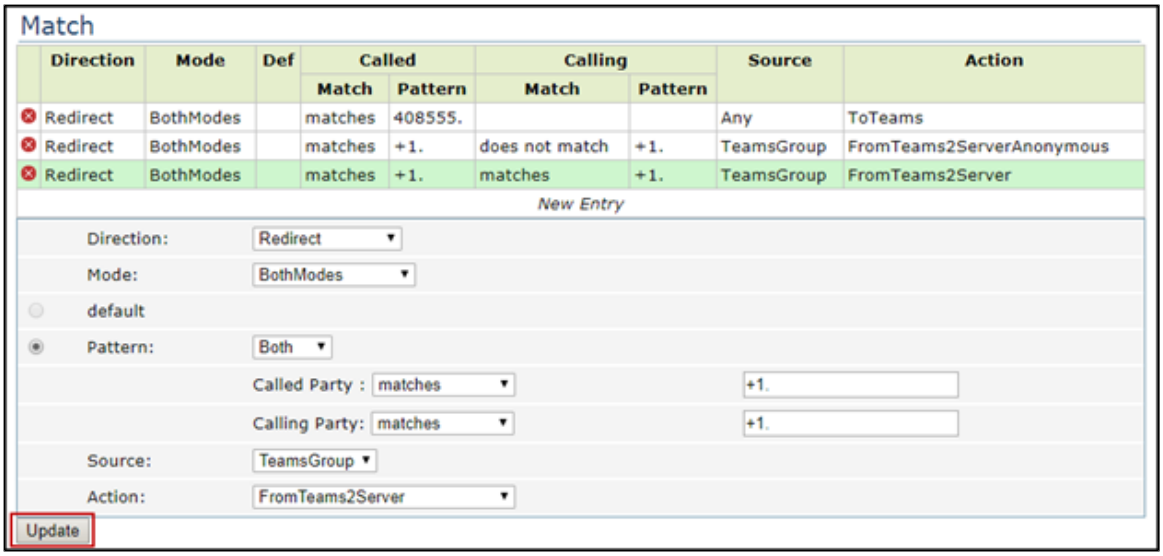
Figure 41: NewEntry3



b) Configure the parameters in the match pane.

c) Click **Update** then Click **Submit** to save the Match.

Figure 42: Add Match From Teams to Server



Configure the From Teams to Server match as follows:

Parameter		Example Configuration Value
Direction:		Redirect
Mode:		BothModes
Default:		Not used for MS-Teams
Pattern:		Both
Called Party:	**Matches**	+1.
Calling Party:	**Matches**	+1.
Source:		TeamsGroup
Action:		FromTeams2Server

You have now completed the Ribbon Communications EdgeMarc configuration for Microsoft Teams and are ready to start testing calls.

The final step is to save the SBC configuration. The configuration can be saved at this point or when you are finished testing.

Save the ESBC Configuration

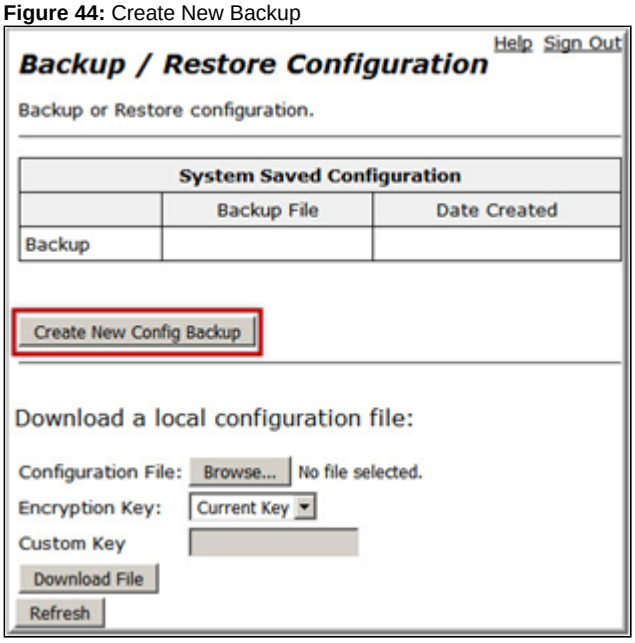
This section discusses how to save the running SBC configuration to restore the system back to a known working configuration if needed.

1. From the left-hand navigation menu select **Admin > Backup/Restore.**

Figure 43: Configuration Menu Backup/Restore

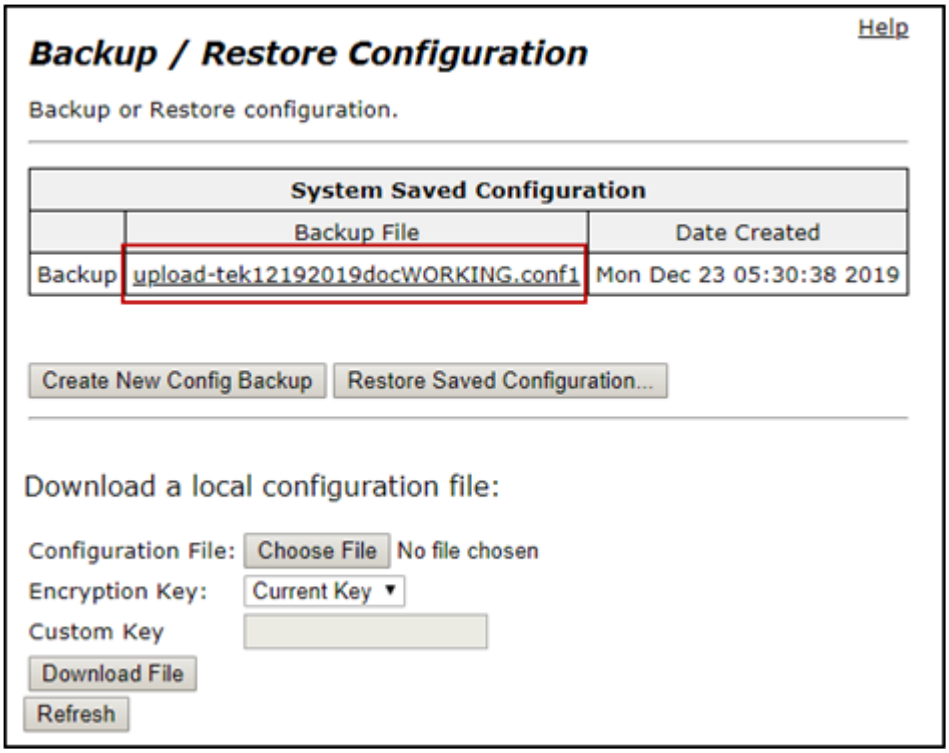
2. Click **Create New Config Backup**. A dialog box will appear, click **OK.**

Figure 44: Create New Backup



3. The system will create a backup file of the current running configuration. Click the file name to download the backup file to the management computer.

Figure 45: Save the Backup to the Management Computer



Section B: Microsoft Teams Configuration

The following Microsoft Teams configurations are included in this section:

1. Configuring Microsoft Teams
2. Obtain IP address and FQDN
3. Domain Name
4. Obtain a Certificate
5. Public Certificate
6. Configure and Generate Certificates on the SBC
7. Configure Office 365 Tenant Voice Routing

Configuring Microsoft Teams

Microsoft Teams Direct Routing Configuration.

Consult the Microsoft documentation for detailed information on Direct Routing interface configuration guidelines, including the RFC standards and the syntax of SIP messages.

Obtain IP Address and FQDN

Requirements for configuring the SBC in support of Teams Direct Routing include:

Requirement	How it is used
Public IP address of NAT device (must be Static)* **Private IP address of the SBC**	Required for SBC Behind the NAT deployment.
Public IP address of SBC	Required for SBC with Public IP deployment.
Public FQDN	The Public FQDN must point to the Public IP Address.

*NAT translates a public IP address to a Private IP address.

Domain Name

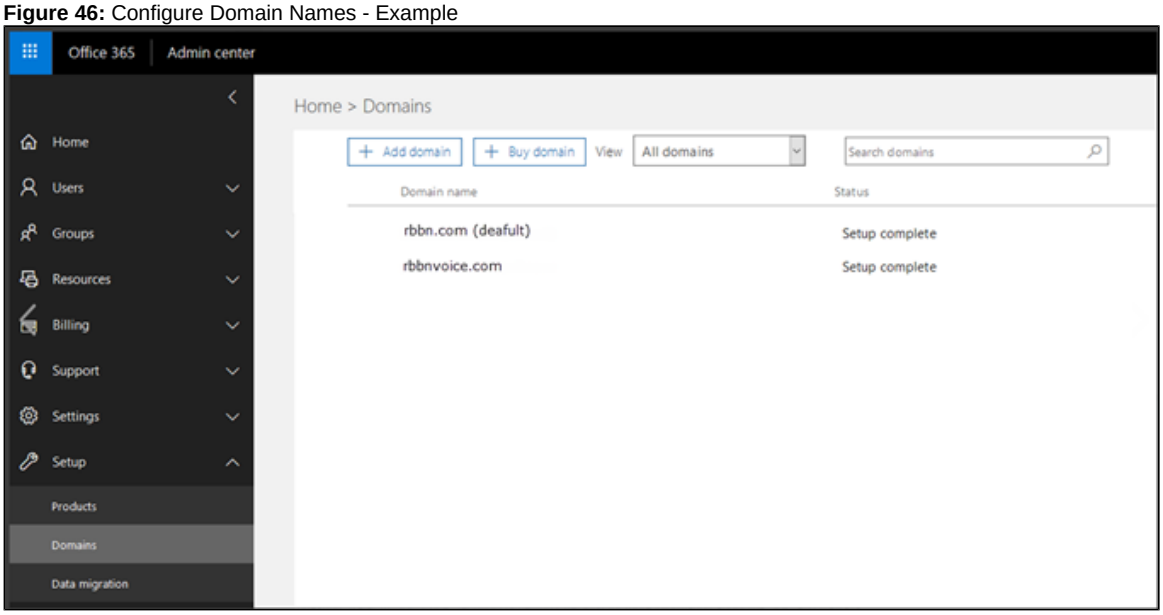
For the SBC to pair with Microsoft Teams, the SBC FQDN domain name must match a name registered in both the **Domains** and **DomainUrlMap** fields of the Tenant. Verify the correct domain name is configured for the Tenant as follows:

1. On the Microsoft Teams Tenant side, execute **Get-CsTenant**.
2. Review the output.
3. Verify that the Domain Name configured is listed in the **Domains** and **DomainUrlMap** attributes for the Tenant. If the Domain Name is incorrect or missing, the SBC will not pair with Microsoft Teams.

Users may be from any SIP domain registered for the tenant. For example, you can configure user **user@example.com** with the SBC FQDN name **sbc2.examplevoice.com**, as long as both names are registered for the tenant.

Domain Name	Use for SBC FQDN	FQDN names - Examples	IPv4 Address
rbbn.com	✔	Valid names: sbc1.rbbn.com	203.0.113.100
rbbnvoice.com	✔	Valid names: · sbc2.rbbnvoice.com · emea.rbbnvoice.com · apac.rbbnvoice.com Non-Valid name; sbc2.emea.rbbnvoice.com (requires registering domain name **emea.rbbnvoice.com** in “Domains” first)	

Figure 46: Configure Domain Names - Example



Obtain a Certificate

Public Certificate

The Certificate must be issued by one of the supported certification authorities (CAs). Wildcard certificates are supported.

• Refer to Microsoft documentation for the supported CAs.
• Refer to Domain Name for certificate Common name formats.

Configure and Generate Certificates on the SBC

Microsoft Teams Direct Routing allows only TLS connections from the SBC for SIP traffic with a certificate signed by one of the trusted certification authorities.

Request a certificate for the SBC External interface and configure it based on the example using GlobalSign as follows:

- Generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority.
- Import the Public CA Root/Intermediate Certificate on the SBC.
- Import the Microsoft CA Certificate on the SBC.
- Import the SBC Certificate.

The certificate is obtained through the Certificate Signing Request (instructions below). The Trusted Root and Intermediary Signing Certificates are obtained from your certification authority.

Configure Office 365 Tenant Voice Routing

A Tenant is used within the Microsoft environment as a single independent enterprise that has subscribed to Office 365 services. Through this tenant, administrators can manage projects, users, and roles. Access the Tenant configuration and configure as detailed below. (For details on accessing the Tenant, refer to Microsoft Teams Documentation).

1. Create Online PSTN Gateway that points to the SBC:
    a. Enter the **SBC FQDN** (Example below: sbc1.rbbn.com). The FQDN must be configured for the Tenant in both the **Domains** and the **DomainUrlMap** fields.
    b. Enter the **SBC SIP Port** (Example below - SipPort5061).

```
New-CsOnlinePSTNGateway -Fqdn sbc1.rbbn.com -SipSignallingPort SipPort5061 -MaxConcurrentSessions
<Max Concurrent Session which SBC capable handling> -Enabled $true
```

2. Configure Teams usage for the user:
    a. Enter the User Identity (Example below: -user1@domain.com)

```
Get-CsOnlineUser -Identity user1@domain.com Set-CsUser -Identity user1@domain.com -EnterpriseVoiceEnabled $true -
HostedVoiceMail $true -OnPremLineURI tel:+10001001008

Grant-CsOnlineVoiceRoutingPolicy -PolicyName "GeneralVRP" -Identity user1@domain.com

Grant-CsTeamsCallingPolicy -PolicyName AllowCalling -Identity user1@domain.com

Grant-CsTeamsUpgradePolicy -PolicyName UpgradeToTeams -Identity user1@domain.com
```