Ribbon EdgeMarc 6000 configuration Microsoft Teams

Table of Contents

Document Overview

This document provides a configuration guide for Ribbon EdgeMarc 6000 when connecting to MS Teams.

This configuration guide supports features given in the Virgin Media SIP Trunk Application.

- For additional information on MS Teams, visit https://docs.microsoft.com/en-us/microsoftteams/
- For additional information on Ribbon SBC, visit https://ribboncommunications.com/

Introduction

The interoperability compliance testing focuses on verifying inbound and outbound call flows between Ribbon EdgeMarc 6000 and MS Teams platform.

Audience

This is a technical document intended for telecommunications engineers for configuring both the Ribbon SBCs and the third-party product. Users will perform steps to navigate the third-party product as well as the Ribbon SBC Command Line Interface (CLI). Understanding the basic concepts of TCP/UDP/TLS, IP/Routing and SIP/RTP is also necessary for completing the configuration and for troubleshooting, if necessary.

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.

Requirements

The following equipment and software were used for the sample configuration:

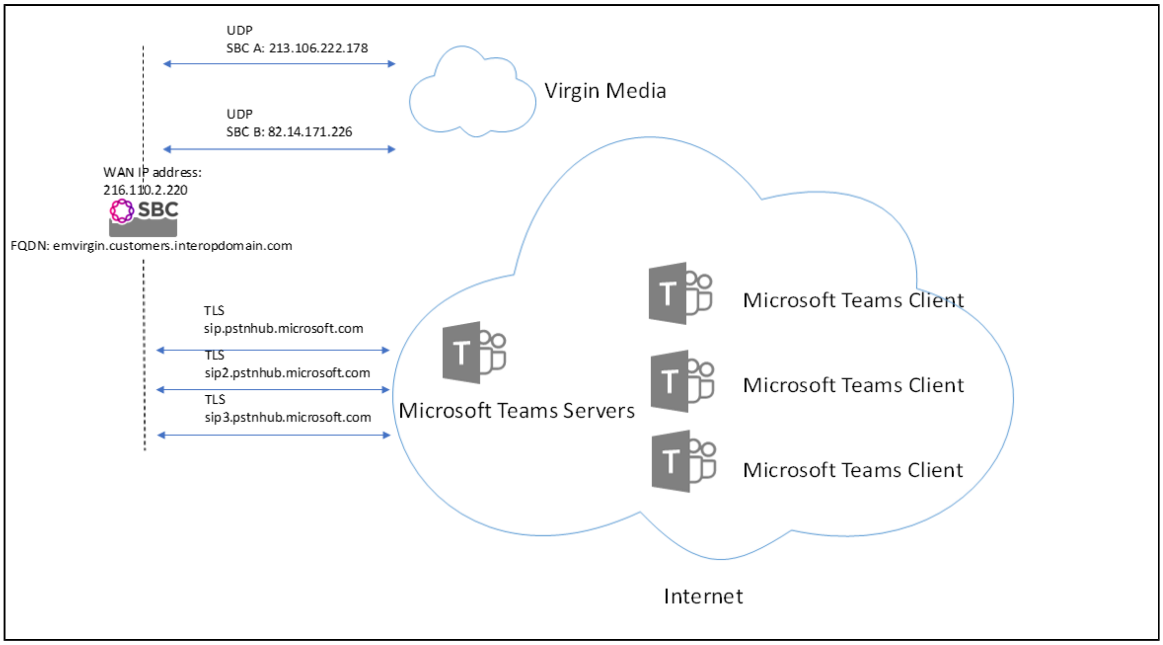
Table 1: Requirements

	Equipment	**Software Version**
Ribbon Communications	Ribbon EdgeMarc 6000	V16.0.0
Third-party Equipment	MS Teams client	1.3.00.28779
	NGT Lite	v.1.51

Reference Configuration

The following reference configuration shows the connectivity between the third-party and Ribbon EdgeMarc 6000.

Figure 1: Reference Configuration



Support

For any questions regarding this document or its content, contact your maintenance and support provider.

Third-Party Product Features

Ribbon supports the following third-party product features:

- Basic originated and terminated calls
- Basic inbound and outbound calls
- Hold and Resume
- Call Forwarding
- DTMF
- Conference Call
- Action on eSBC outage (restart of eSBC)
- Action on Loss of Virgin Media primary SBC

Configure Microsoft Teams

The following new configurations are included in this section:

1. Microsoft Teams Direct Routing Configuration
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

1. Microsoft Teams Direct Routing Configuration

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

2. Obtain IP address and FQDN

The following table provides the requirements for configuring the SBC to support Teams Direct Routing:

Table1 : SBC Requirements

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.

3. Domain Name

For the SBC to pair with Microsoft Teams, ensure that the SBC FQDN domain name matches with the name registered in both the **Domains** and **DomainUrlMap** fields of the Tenant.

Follow the steps to verify that the correct domain name is configured for the Tenant:

1. On the Microsoft Teams Tenant side, execute **Get-CsTenant**.
2. Review the output.
3. Verify that the configured Domain Name 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.

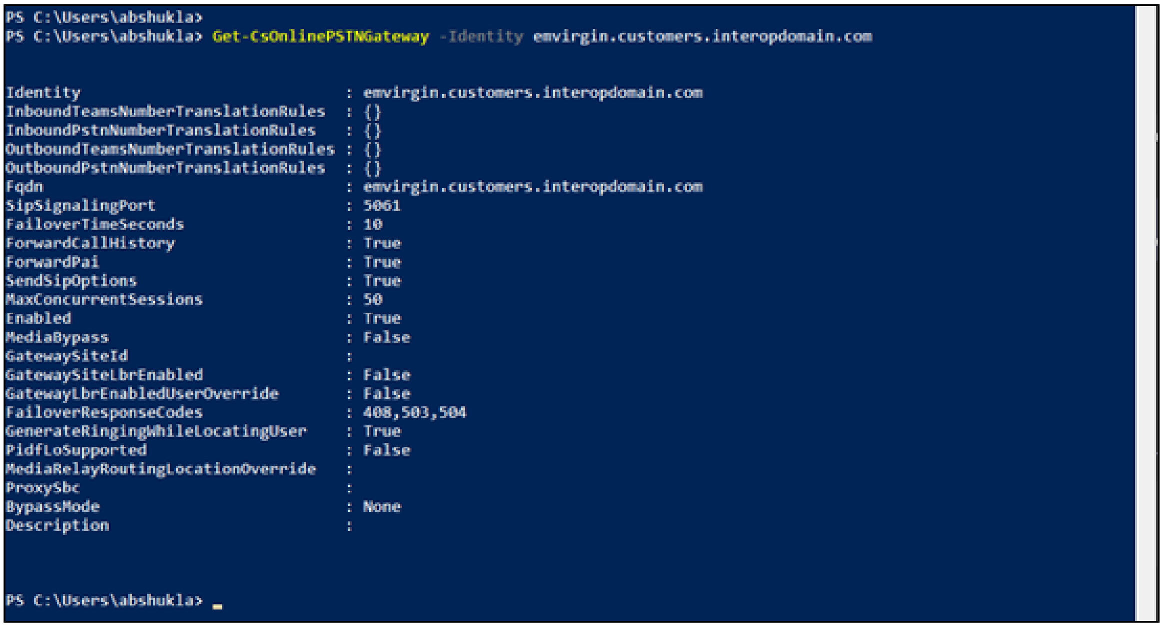
You can configure users from any SIP domain registered for the tenant. For example, you can configure user **user@example.com** with the SBC FQDN name **sbc2.examplevoice.com**, as long as both names are registered for the tenant.

Table 2: Domain Name Examples

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 Invalid name: • sbc2.emea.rbbnvoice.com (This requires registering the domain name **emea.rbbnvoice.com** in “Domains” first.)	-

Configure Domain Names - Example :

Figure 2: Domain Names



```
PS C:\Users\abshukla>
PS C:\Users\abshukla> Get-CsOnlinePSTNGateway -Identity emvirgin.customers.interopdomain.com


Identity                             : emvirgin.customers.interopdomain.com
InboundTeamsNumberTranslationRules   : {}
InboundPstnNumberTranslationRules    : {}
OutboundTeamsNumberTranslationRules  : {}
OutboundPstnNumberTranslationRules   : {}
Fqdn                                 : emvirgin.customers.interopdomain.com
SipSignalingPort                     : 5061
FailoverTimeSeconds                  : 10
ForwardCallHistory                   : True
ForwardPai                           : True
SendSipOptions                       : True
MaxConcurrentSessions                : 50
Enabled                              : True
MediaBypass                          : False
GatewaySiteId                        :
GatewaySiteLbrEnabled                : False
GatewayLbrEnabledUserOverride        : False
FailoverResponseCodes                : 408,503,504
GenerateRingingWhileLocatingUser     : True
PidfLoSupported                      : False
MediaRelayRoutingLocationOverride    :
ProxySbc                             :
BypassMode                           : None
Description                          :



PS C:\Users\abshukla> _
```

4. Obtain a Certificate

5. Public Certificate

Make sure that the certificate is issued by one of the supported certification authorities (CA). Note that wildcard certificates are supported.

- Refer to Microsoft documentation for the supported CAs.
- Refer to Domain Name in Domain Name Examples for certificate common name formats.

6. 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.

Follow the steps to request a certificate for the SBC External interface and configure it based on the example using the GlobalSign:

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

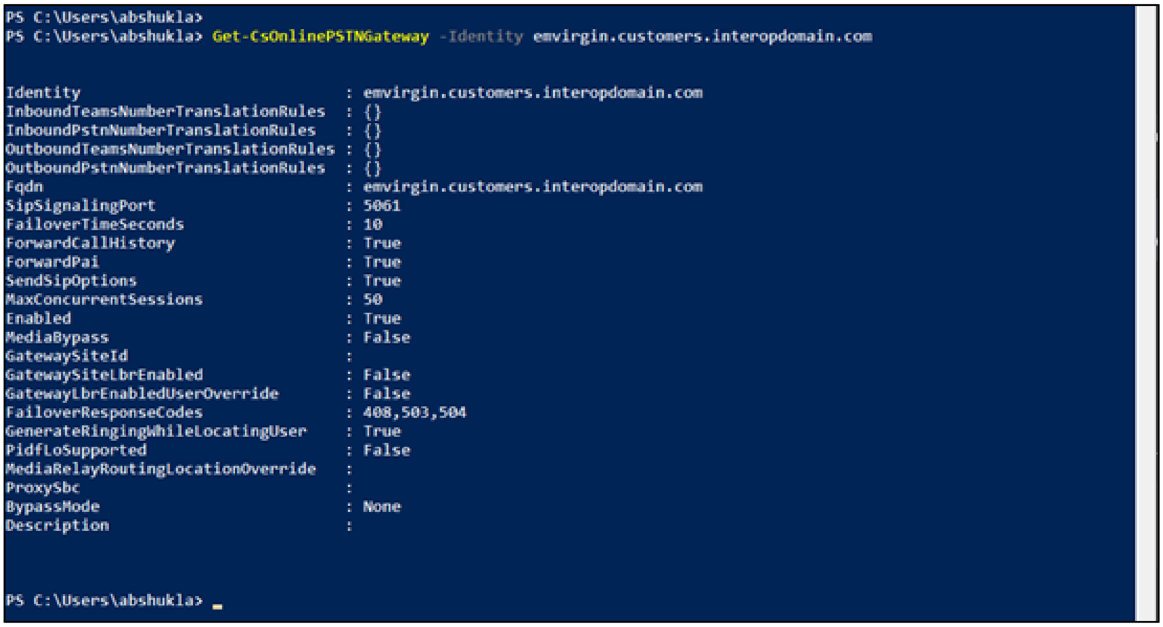
You can obtain the certificate through the Certificate Signing Request (see the following instructions). You can obtain the Trusted Root and Intermediary Signing Certificates from your certification authority.

7. 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. Perform the following steps to configure the Tenant. 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** (see example below - sbc1.rbbn.com). Be sure to configure the FQDN for the Tenant in both the **Domains** and the **DomainUrlMap** fields.
    b. Enter the **SBC SIP Port** (see example below - SipPort5061).

Figure 3: Domain Names

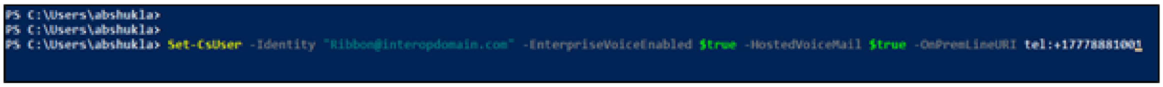


```
PS C:\Users\abshukla>
PS C:\Users\abshukla> Get-CsOnlinePSTNGateway -Identity emvirgin.customers.interopdomain.com


Identity                              : emvirgin.customers.interopdomain.com
InboundTeamsNumberTranslationRules    : {}
InboundPstnNumberTranslationRules     : {}
OutboundTeamsNumberTranslationRules : {}
OutboundPstnNumberTranslationRules    : {}
Fqdn                                  : emvirgin.customers.interopdomain.com
SipSignalingPort                      : 5061
FailoverTimeSeconds                   : 10
ForwardCallHistory                    : True
ForwardPai                            : True
SendSipOptions                        : True
MaxConcurrentSessions                 : 50
Enabled                               : True
MediaBypass                           : False
GatewaySiteId                         :
GatewaySiteLbrEnabled                 : False
GatewayLbrEnabledUserOverride         : False
FailoverResponseCodes                 : 408,503,504
GenerateRingingWhileLocatingUser      : True
PidfLoSupported                       : False
MediaRelayRoutingLocationOverride     :
ProxySbc                              :
BypassMode                            : None
Description                           :



PS C:\Users\abshukla> _
```

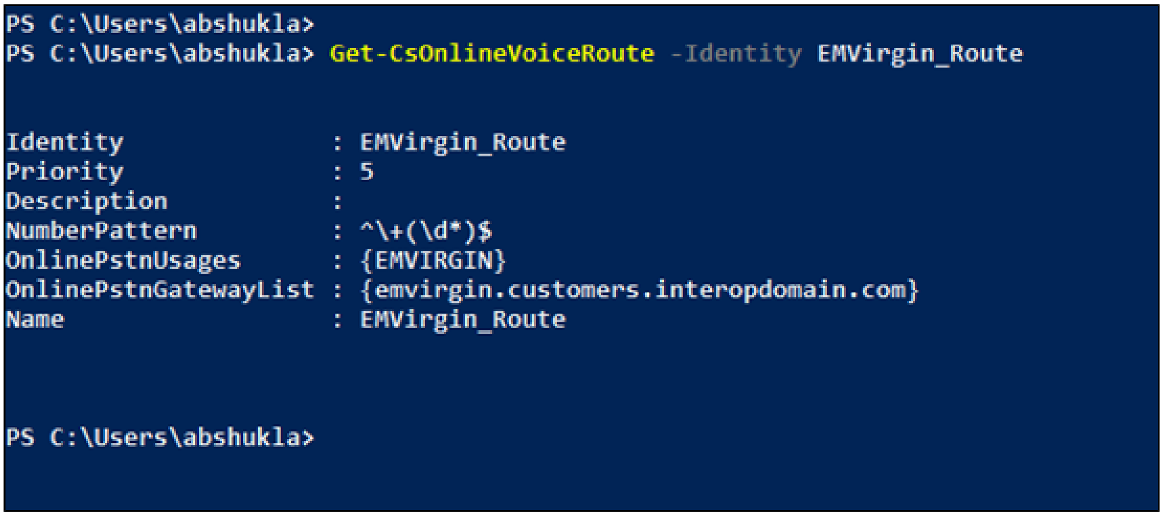
2. Configure Teams usage for the user:

   a. Enter the User Identity (see example below - user1@domain.com)

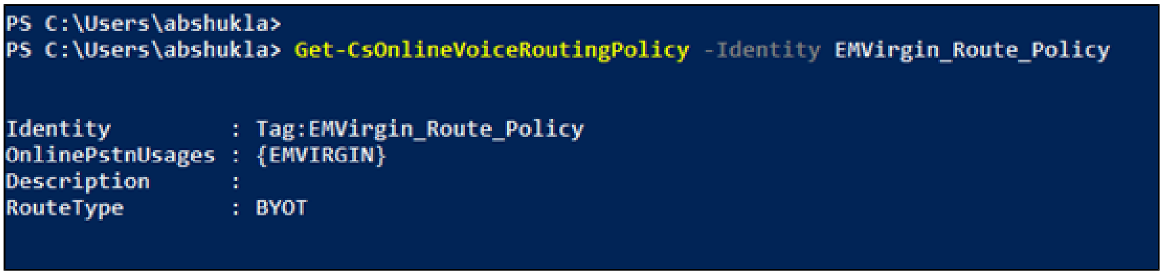
Figure 4: User



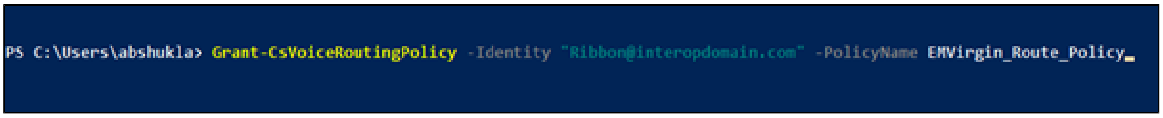
```
PS C:\Users\abshukla>
PS C:\Users\abshukla>
PS C:\Users\abshukla> Set-CsUser -Identity "Ribbon@interopdomain.com" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true -OnPremLineURI tel:+17778881001
```



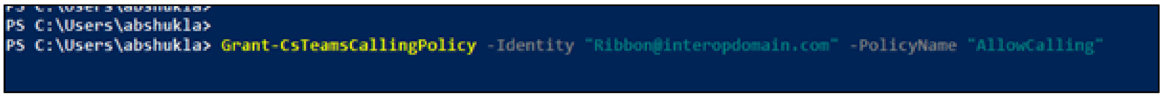
```
PS C:\Users\abshukla>
PS C:\Users\abshukla> Get-CsOnlineVoiceRoute -Identity EMVirgin_Route


Identity                : EMVirgin_Route
Priority                : 5
Description             :
NumberPattern           : ^\+(\d*)$
OnlinePstnUsages        : {EMVIRGIN}
OnlinePstnGatewayList : {emvirgin.customers.interopdomain.com}
Name                    : EMVirgin_Route



PS C:\Users\abshukla>
```



```
PS C:\Users\abshukla>
PS C:\Users\abshukla> Get-CsOnlineVoiceRoutingPolicy -Identity EMVirgin_Route_Policy


Identity         : Tag:EMVirgin_Route_Policy
OnlinePstnUsages : {EMVIRGIN}
Description      :
RouteType        : BYOT
```



```
PS C:\Users\abshukla> Grant-CsVoiceRoutingPolicy -Identity "Ribbon@interopdomain.com" -PolicyName EMVirgin_Route_Policy
```



```
PS C:\Users\abshukla>
PS C:\Users\abshukla>
PS C:\Users\abshukla> Grant-CsTeamsCallingPolicy -Identity "Ribbon@interopdomain.com" -PolicyName "AllowCalling"
```

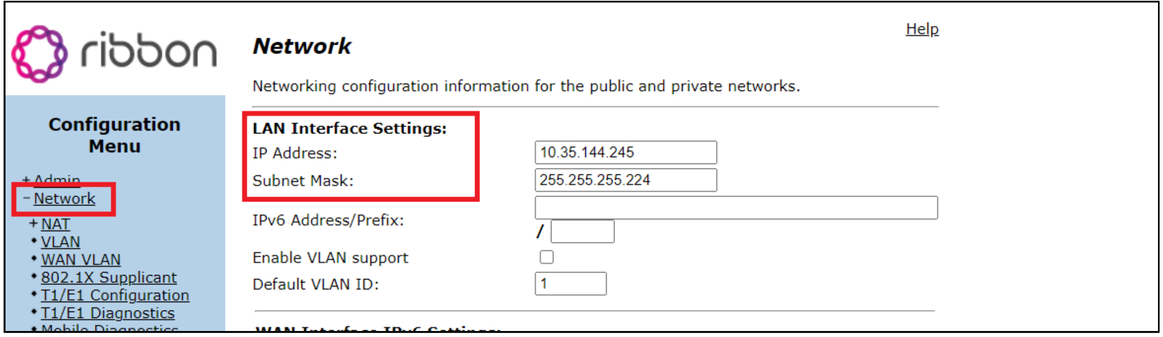
EdgeMarc Configuration

Network

LAN and WAN Interfaces

1. Login to the EdgeMarc as a **root** user.
2. Click *Network* to configure the LAN and WAN interfaces.

Figure 5: EdgeMarc Network LAN Interface



Network

Networking configuration information for the public and private networks.

LAN Interface Settings:

IP Address: 10.35.144.245

Subnet Mask: 255.255.255.224

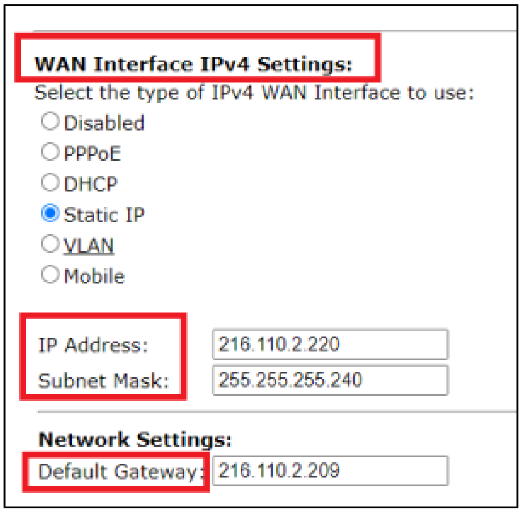
IPv6 Address/Prefix: /

Enable VLAN support ☐

Default VLAN ID: 1

WAN Interface IPv6 Settings:

Figure 6: EdgeMarc Network WAN Interface



WAN Interface IPv4 Settings:

Select the type of IPv4 WAN Interface to use:

- ○ Disabled
- ○ PPPoE
- ○ DHCP
- ● Static IP
- ○ VLAN
- ○ Mobile

IP Address:	216.110.2.220
Subnet Mask:	255.255.255.240

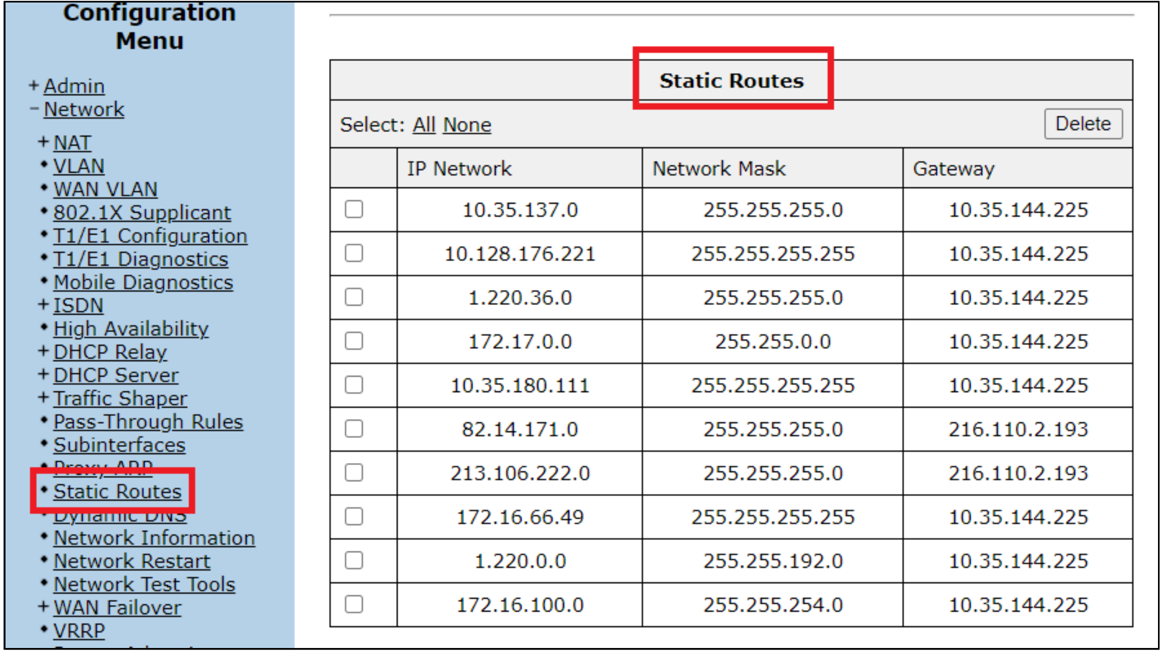
Network Settings:

Default Gateway:	216.110.2.209

Static Routes

Click *Network* > *Static Routes* to configure the routes.

Figure 7: Static Routes



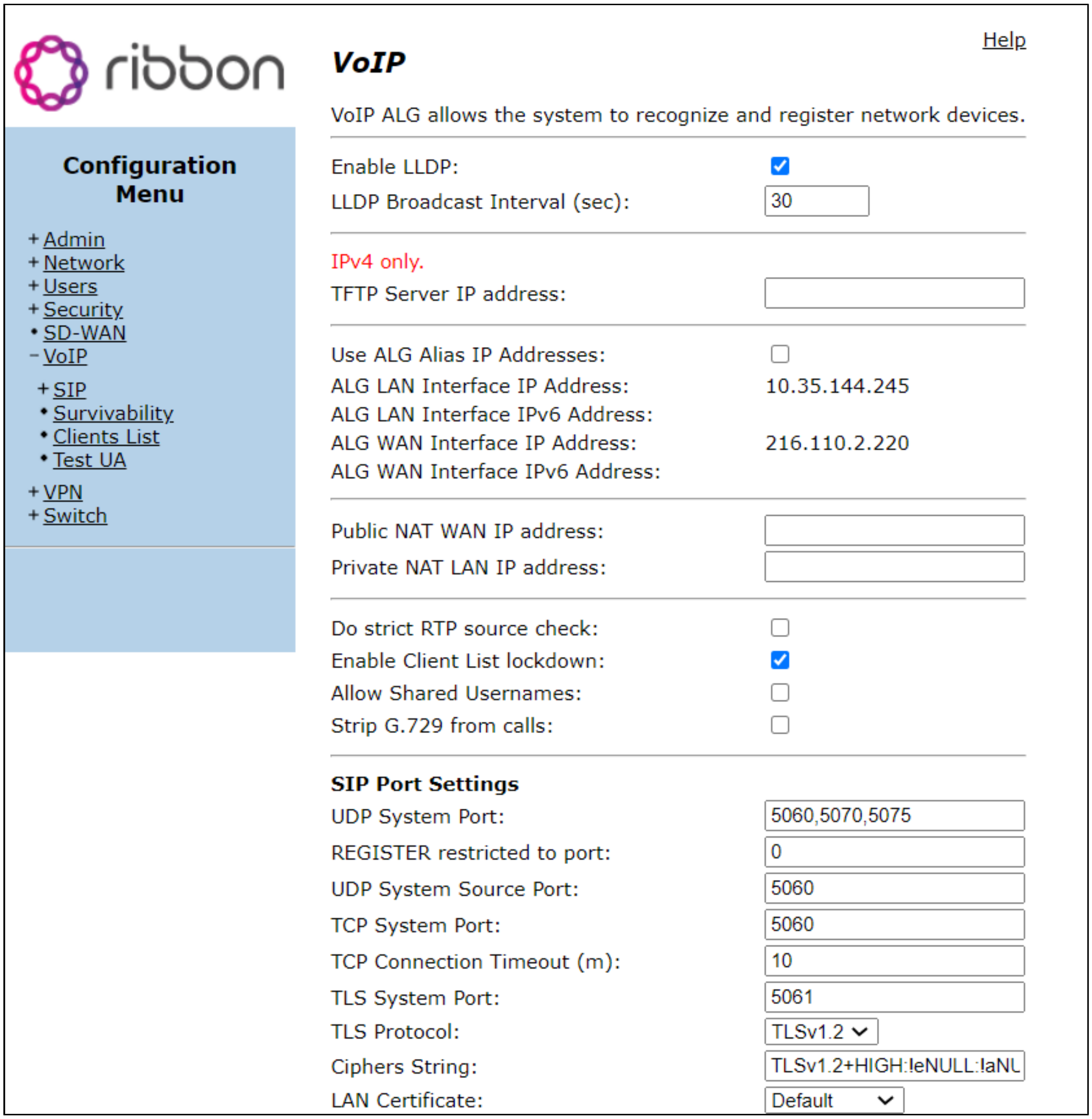
	IP Network	Network Mask	Gateway
□	10.35.137.0	255.255.255.0	10.35.144.225
□	10.128.176.221	255.255.255.255	10.35.144.225
□	1.220.36.0	255.255.255.0	10.35.144.225
□	172.17.0.0	255.255.0.0	10.35.144.225
□	10.35.180.111	255.255.255.255	10.35.144.225
□	82.14.171.0	255.255.255.0	216.110.2.193
□	213.106.222.0	255.255.255.0	216.110.2.193
□	172.16.66.49	255.255.255.255	10.35.144.225
□	1.220.0.0	255.255.192.0	10.35.144.225
□	172.16.100.0	255.255.254.0	10.35.144.225

VoIP

VoIP Settings

1. Login as a **root** user.
2. Click *VoIP* to configure the VoIP features.

Figure 8: VoIP



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:

Use ALG Alias IP Addresses: □

ALG LAN Interface IP Address: 10.35.144.245

ALG LAN Interface IPv6 Address:

ALG WAN Interface IP Address: 216.110.2.220

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: □

SIP Port Settings

UDP System Port: 5060,5070,5075

REGISTER restricted to port: 0

UDP System Source Port: 5060

TCP System Port: 5060

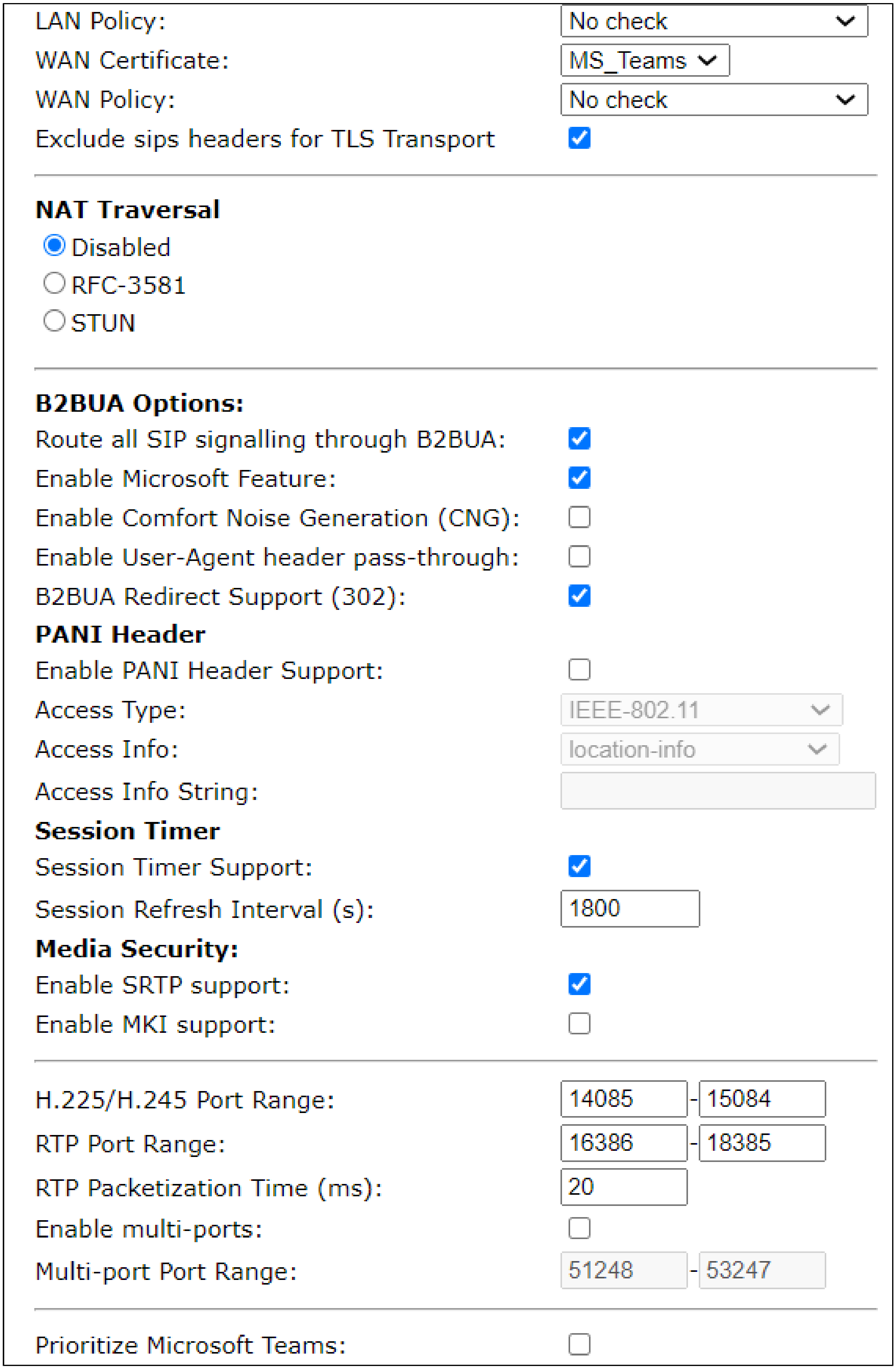
TCP Connection Timeout (m): 10

TLS System Port: 5061

TLS Protocol: TLSv1.2

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

LAN Certificate: Default



LAN Policy:	No check
WAN Certificate:	MS_Teams
WAN Policy:	No check
Exclude sips headers for TLS Transport	☑

NAT Traversal

● Disabled
○ RFC-3581
○ STUN

B2BUA Options:

Route all SIP signalling through B2BUA:	☑
Enable Microsoft Feature:	☑
Enable Comfort Noise Generation (CNG):	□
Enable User-Agent header pass-through:	□
B2BUA Redirect Support (302):	☑

PANI Header

Enable PANI Header Support:	□
Access Type:	IEEE-802.11
Access Info:	location-info
Access Info String:	

Session Timer

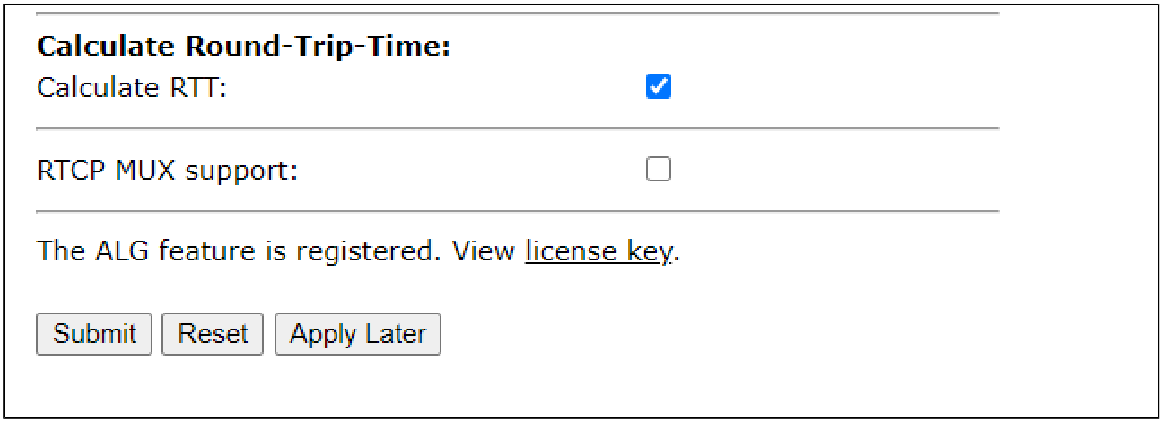
Session Timer Support:	☑
Session Refresh Interval (s):	1800

Media Security:

Enable SRTP support:	☑
Enable MKI support:	□

H.225/H.245 Port Range:	14085 - 15084
RTP Port Range:	16386 - 18385
RTP Packetization Time (ms):	20
Enable multi-ports:	□
Multi-port Port Range:	51248 - 53247

Prioritize Microsoft Teams:	□



Calculate Round-Trip-Time:

Calculate RTT: ☑

RTCP MUX support: □

The ALG feature is registered. View license key.

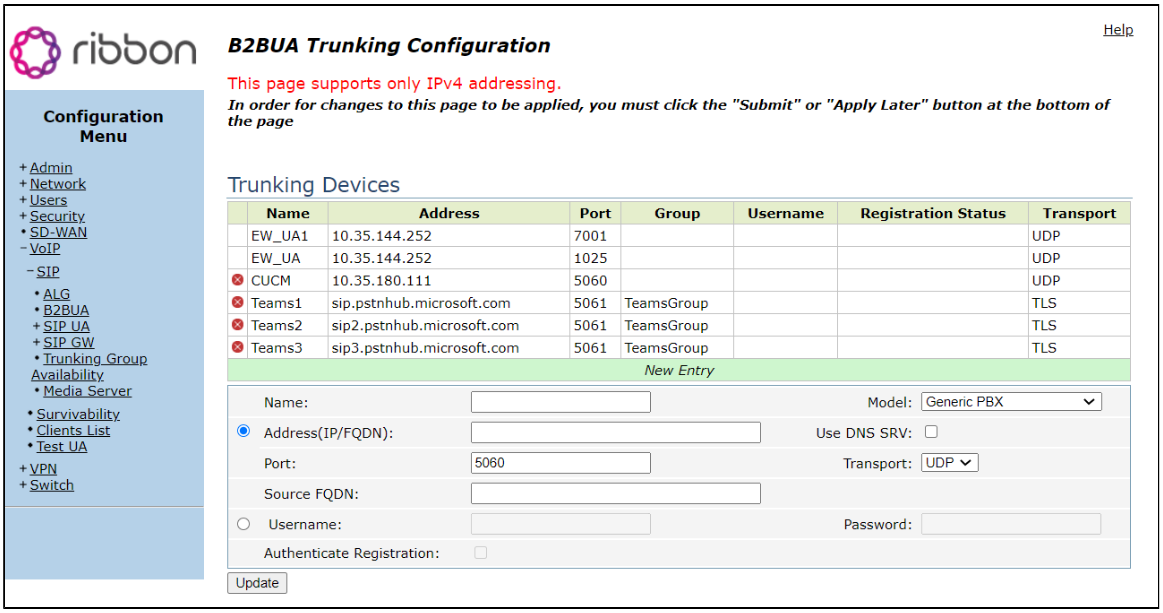
SIP Settings

1. Click *VoIP* > *SIP* to configure the SIP settings.
2. Configure the SIP servers.

B2BUA

1. Click *VoIP* > *B2BUA* for B2BUA trunking configuration.
2. Configure the LAN Part with the next form.

Figure 9: B2BUA



B2BUA Trunking Configuration

This page supports only IPv4 addressing.

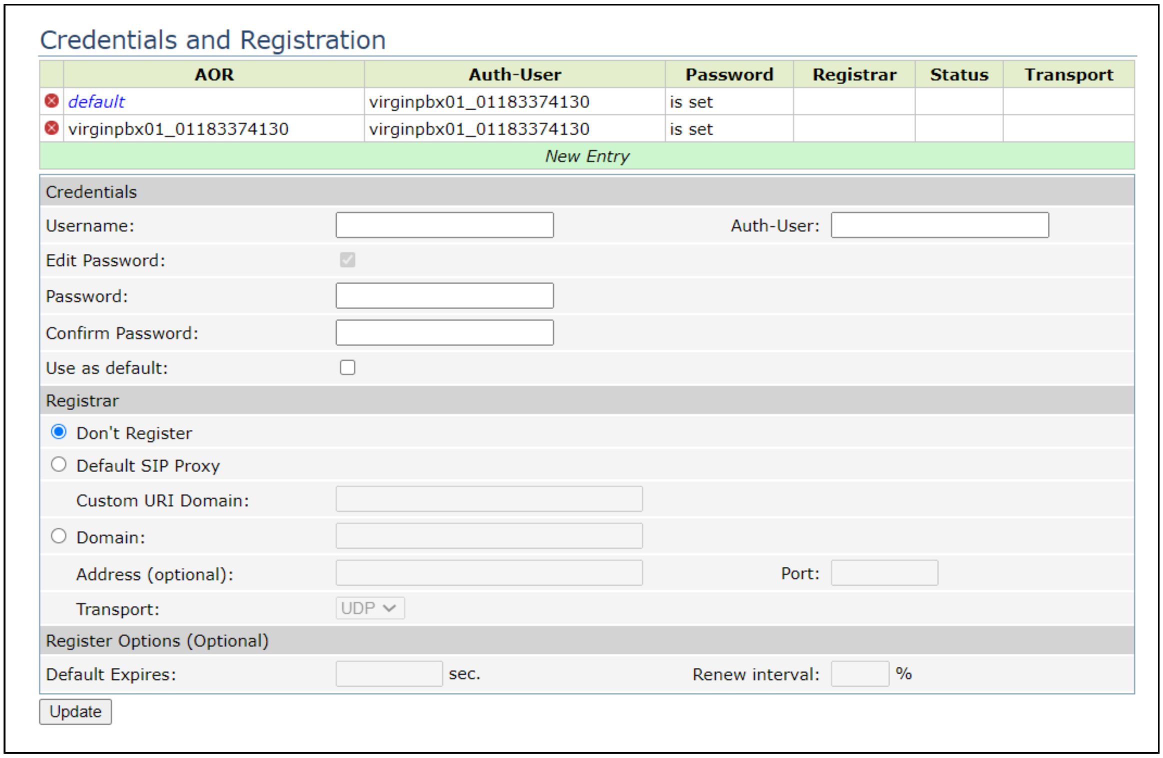
In order for changes to this page to be applied, you must click the "Submit" or "Apply Later" button at the bottom of the page

Trunking Devices

	Name	Address	Port	Group	Username	Registration Status	Transport
	EW_UA1	10.35.144.252	7001				UDP
	EW_UA	10.35.144.252	1025				UDP
⊗	CUCM	10.35.180.111	5060				UDP
⊗	Teams1	sip.pstnhub.microsoft.com	5061	TeamsGroup			TLS
⊗	Teams2	sip2.pstnhub.microsoft.com	5061	TeamsGroup			TLS
⊗	Teams3	sip3.pstnhub.microsoft.com	5061	TeamsGroup			TLS

New Entry

	Name:		Model:	Generic PBX
●	Address(IP/FQDN):		Use DNS SRV:	□
	Port:	5060	Transport:	UDP
	Source FQDN:			
○	Username:		Password:	
	Authenticate Registration:	□		



Credentials and Registration

	AOR	Auth-User	Password	Registrar	Status	Transport
☒	*default*	virginpbx01_01183374130	is set			
☒	virginpbx01_01183374130	virginpbx01_01183374130	is set			
	New Entry					

Credentials

Username:		Auth-User:	
Edit Password:	☑		
Password:			
Confirm Password:			
Use as default:	□		

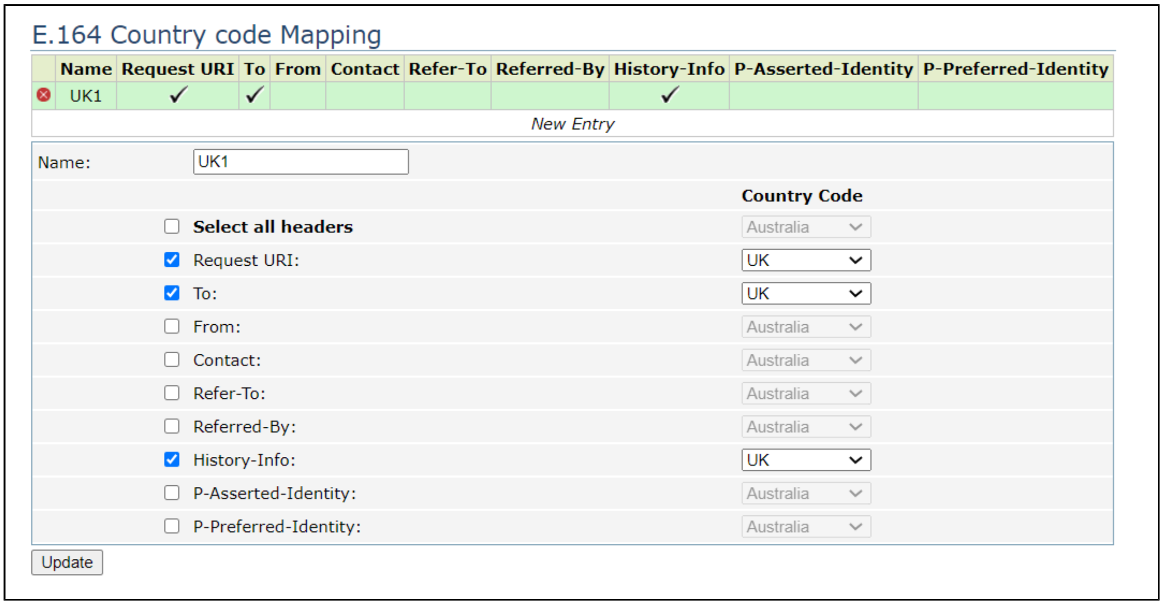
Registrar

● Don't Register			
○ Default SIP Proxy			
Custom URI Domain:			
○ Domain:			
Address (optional):		Port:	
Transport:	UDP		

Register Options (Optional)

Default Expires:	sec.	Renew interval:	%

Update



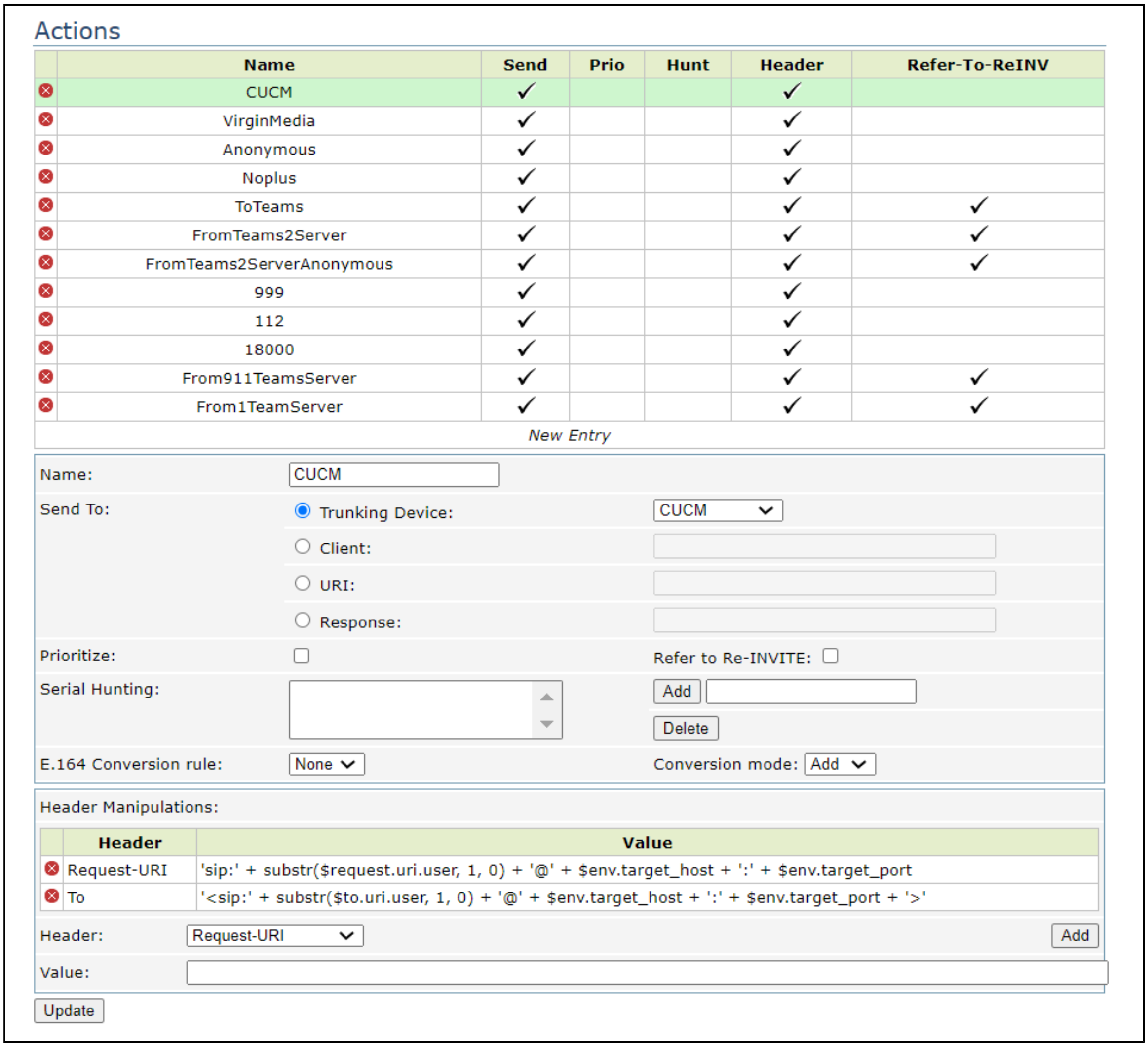
E.164 Country code Mapping

	Name	Request URI	To	From	Contact	Refer-To	Referred-By	History-Info	P-Asserted-Identity	P-Preferred-Identity
☒	UK1	✓	✓					✓		
	New Entry									

Name: UK1

	Country Code
□ **Select all headers**	Australia
☑ Request URI:	UK
☑ To:	UK
□ From:	Australia
□ Contact:	Australia
□ Refer-To:	Australia
□ Referred-By:	Australia
☑ History-Info:	UK
□ P-Asserted-Identity:	Australia
□ P-Preferred-Identity:	Australia

Update



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
⊗	CUCM	✓			✓	
⊗	VirginMedia	✓			✓	
⊗	Anonymous	✓			✓	
⊗	Noplus	✓			✓	
⊗	ToTeams	✓			✓	✓
⊗	FromTeams2Server	✓			✓	✓
⊗	FromTeams2ServerAnonymous	✓			✓	✓
⊗	999	✓			✓	
⊗	112	✓			✓	
⊗	18000	✓			✓	
⊗	From911TeamsServer	✓			✓	✓
⊗	From1TeamServer	✓			✓	✓

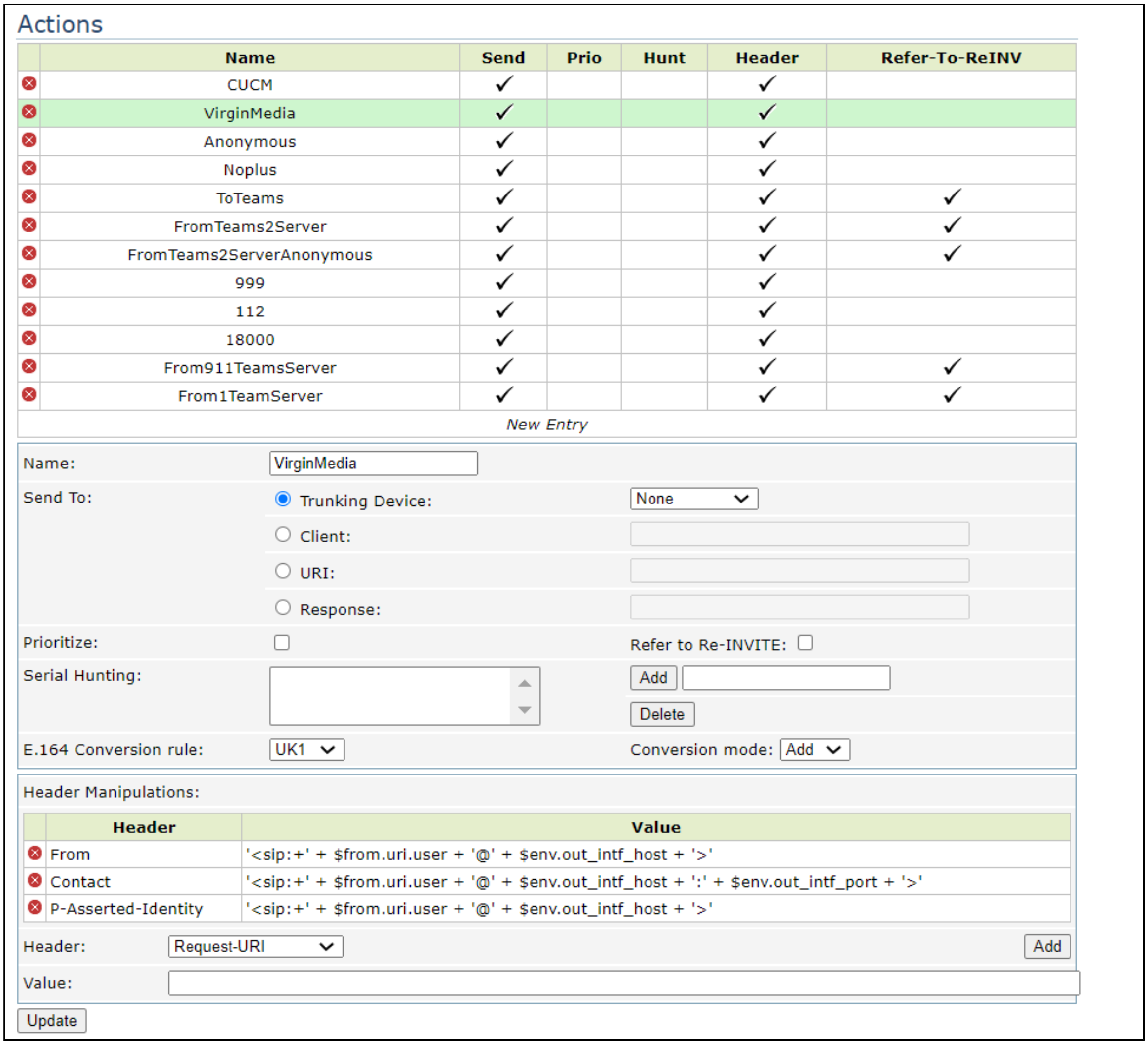
New Entry

Name:	CUCM	
Send To:	● Trunking Device:	CUCM
	○ Client:	
	○ URI:	
	○ Response:	
Prioritize:	□	Refer to Re-INVITE: □
Serial Hunting:		Add
		Delete
E.164 Conversion rule:	None	Conversion mode: Add

Header Manipulations:

	Header	Value
⊗	Request-URI	'sip:' + substr($request.uri.user, 1, 0) + '@' + $env.target_host + ':' + $env.target_port
⊗	To	'<sip:' + substr($to.uri.user, 1, 0) + '@' + $env.target_host + ':' + $env.target_port + '>'

Header:	Request-URI	Add
Value:		



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
⊗	CUCM	✓			✓	
⊗	VirginMedia	✓			✓	
⊗	Anonymous	✓			✓	
⊗	Noplus	✓			✓	
⊗	ToTeams	✓			✓	✓
⊗	FromTeams2Server	✓			✓	✓
⊗	FromTeams2ServerAnonymous	✓			✓	✓
⊗	999	✓			✓	
⊗	112	✓			✓	
⊗	18000	✓			✓	
⊗	From911TeamsServer	✓			✓	✓
⊗	From1TeamServer	✓			✓	✓

New Entry

Name:	VirginMedia		
Send To:	● Trunking Device:	None	
	○ Client:		
	○ URI:		
	○ Response:		
Prioritize:	□	Refer to Re-INVITE: □	
Serial Hunting:		Add	
		Delete	
E.164 Conversion rule:	UK1	Conversion mode: Add	

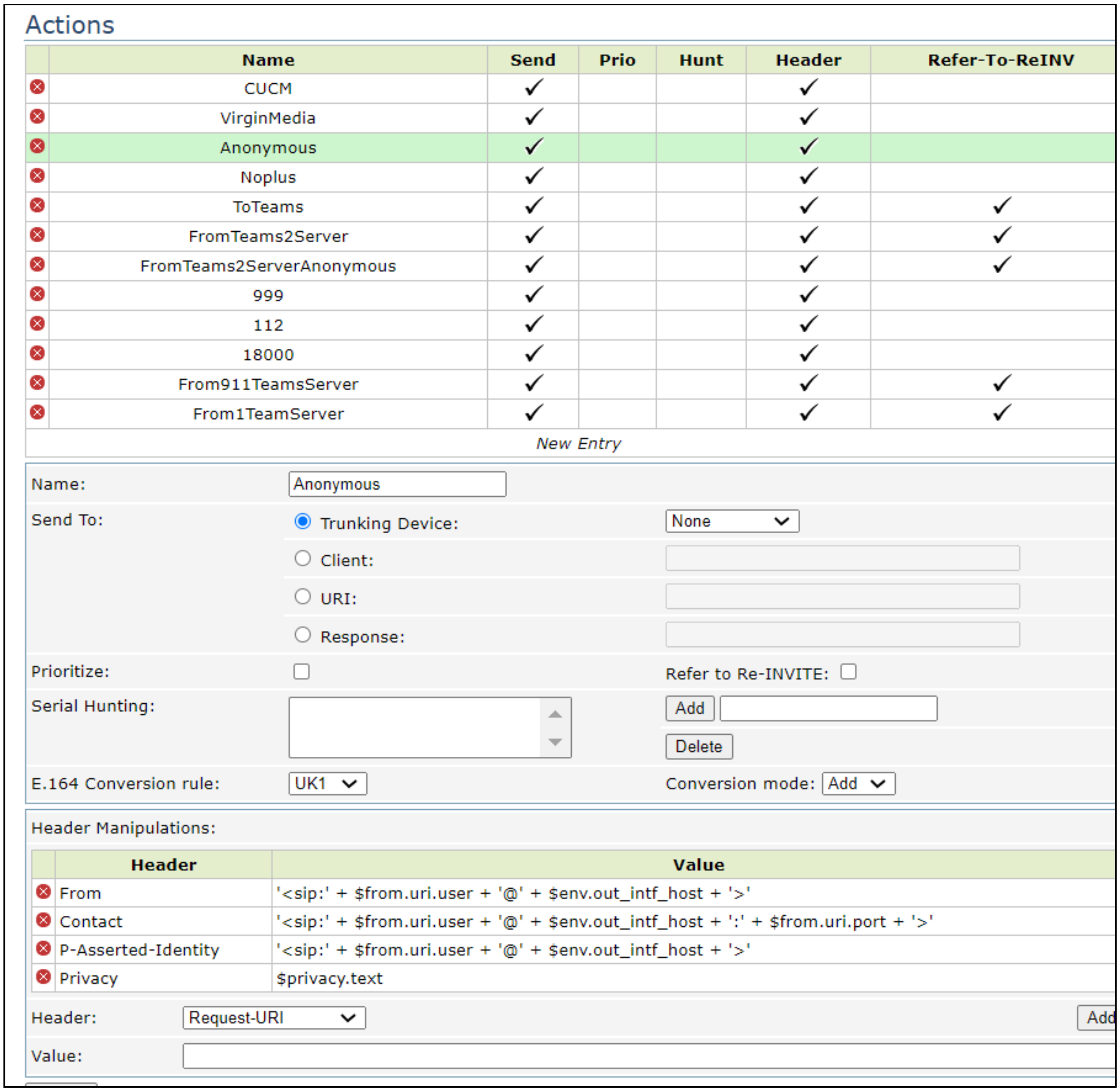
Header Manipulations:

	Header	Value
⊗	From	'<sip:+' + $from.uri.user + '@' + $env.out_intf_host + '>'
⊗	Contact	'<sip:+' + $from.uri.user + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>'
⊗	P-Asserted-Identity	'<sip:+' + $from.uri.user + '@' + $env.out_intf_host + '>'

Header: Request-URI Add

Value:

Update



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
⊗	CUCM	✓			✓	
⊗	VirginMedia	✓			✓	
⊗	Anonymous	✓			✓	
⊗	Noplus	✓			✓	
⊗	ToTeams	✓			✓	✓
⊗	FromTeams2Server	✓			✓	✓
⊗	FromTeams2ServerAnonymous	✓			✓	✓
⊗	999	✓			✓	
⊗	112	✓			✓	
⊗	18000	✓			✓	
⊗	From911TeamsServer	✓			✓	✓
⊗	From1TeamServer	✓			✓	✓

New Entry

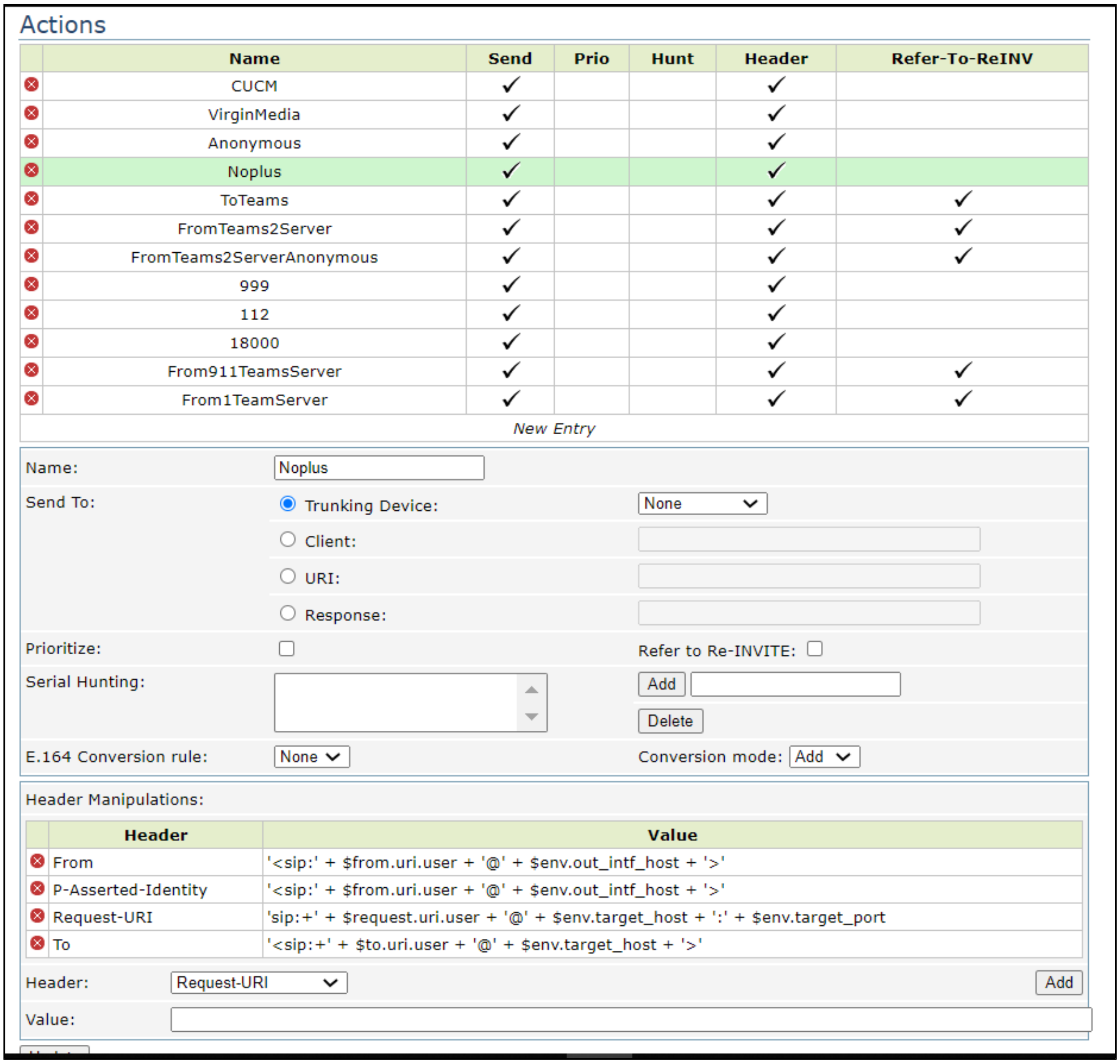
Name:	Anonymous	
Send To:	● Trunking Device:	None
	○ Client:	
	○ URI:	
	○ Response:	
Prioritize:	□	Refer to Re-INVITE: □
Serial Hunting:		Add Delete
E.164 Conversion rule:	UK1	Conversion mode: Add

Header Manipulations:

	Header	Value
⊗	From	'<sip:' + $from.uri.user + '@' + $env.out_intf_host + '>'
⊗	Contact	'<sip:' + $from.uri.user + '@' + $env.out_intf_host + ':' + $from.uri.port + '>'
⊗	P-Asserted-Identity	'<sip:' + $from.uri.user + '@' + $env.out_intf_host + '>'
⊗	Privacy	$privacy.text

Header: Request-URI Add

Value:



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
⊗	CUCM	✓			✓	
⊗	VirginMedia	✓			✓	
⊗	Anonymous	✓			✓	
⊗	Noplus	✓			✓	
⊗	ToTeams	✓			✓	✓
⊗	FromTeams2Server	✓			✓	✓
⊗	FromTeams2ServerAnonymous	✓			✓	✓
⊗	999	✓			✓	
⊗	112	✓			✓	
⊗	18000	✓			✓	
⊗	From911TeamsServer	✓			✓	✓
⊗	From1TeamServer	✓			✓	✓

New Entry

Name: Noplus

Send To:
- ● Trunking Device: None
- ○ Client:
- ○ URI:
- ○ Response:

Prioritize: □ Refer to Re-INVITE: □

Serial Hunting:

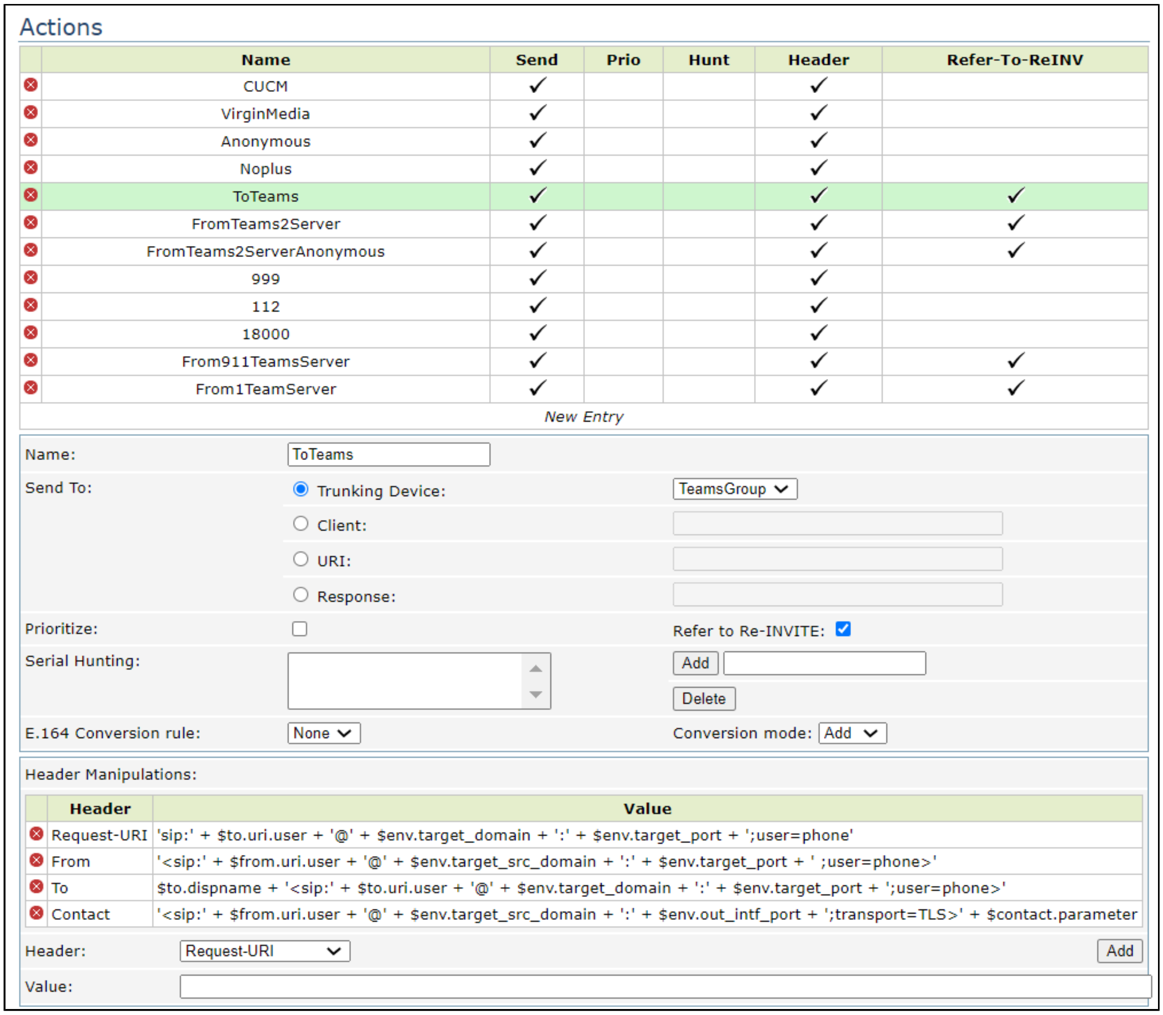
E.164 Conversion rule: None Conversion mode: Add

Header Manipulations:

	Header	Value
⊗	From	'<sip:' + $from.uri.user + '@' + $env.out_intf_host + '>'
⊗	P-Asserted-Identity	'<sip:' + $from.uri.user + '@' + $env.out_intf_host + '>'
⊗	Request-URI	'sip:+' + $request.uri.user + '@' + $env.target_host + ':' + $env.target_port
⊗	To	'<sip:+' + $to.uri.user + '@' + $env.target_host + '>'

Header: Request-URI

Value:



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
⊗	CUCM	✓			✓	
⊗	VirginMedia	✓			✓	
⊗	Anonymous	✓			✓	
⊗	Noplus	✓			✓	
⊗	ToTeams	✓			✓	✓
⊗	FromTeams2Server	✓			✓	✓
⊗	FromTeams2ServerAnonymous	✓			✓	✓
⊗	999	✓			✓	
⊗	112	✓			✓	
⊗	18000	✓			✓	
⊗	From911TeamsServer	✓			✓	✓
⊗	From1TeamServer	✓			✓	✓

New Entry

Name: ToTeams

Send To:
● Trunking Device: TeamsGroup
○ Client:
○ URI:
○ Response:

Prioritize: □

Refer to Re-INVITE: ☑

Serial Hunting:

Add

Delete

E.164 Conversion rule: None

Conversion mode: Add

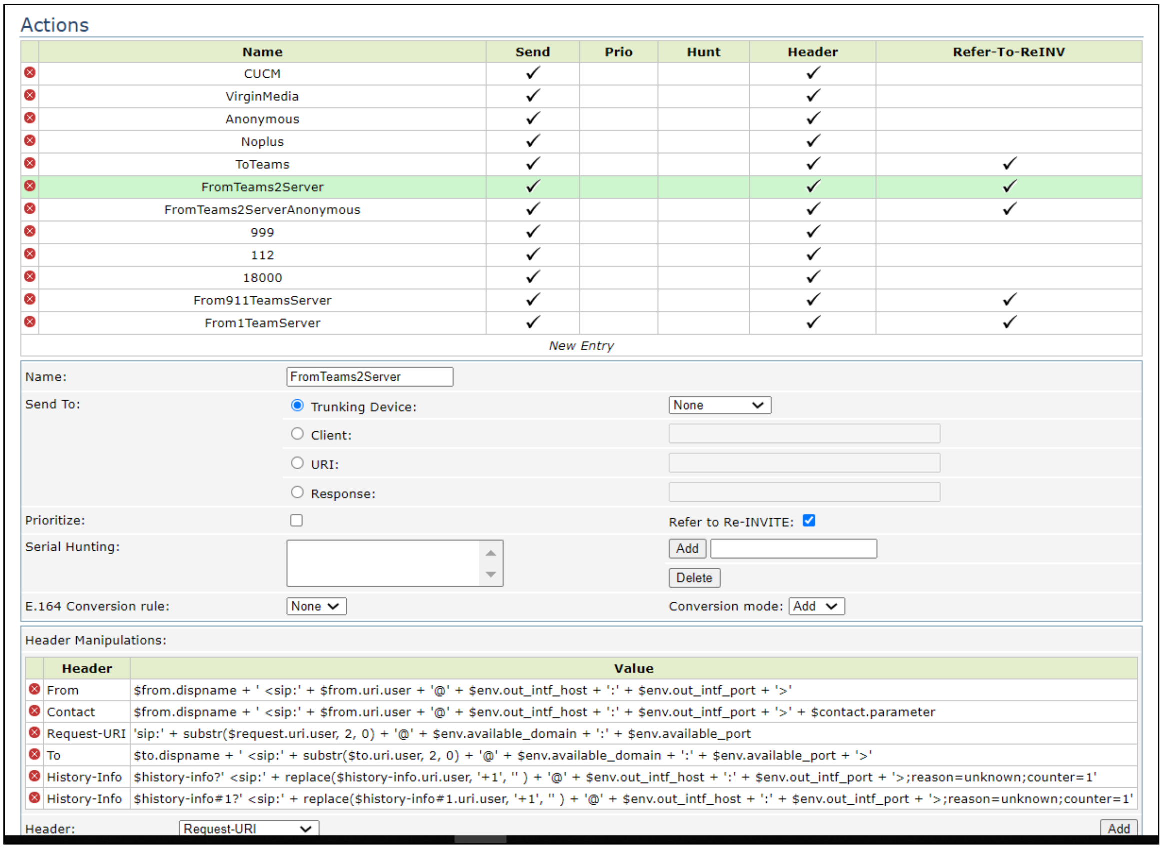
Header Manipulations:

	Header	Value
⊗	Request-URI	'sip:' + $to.uri.user + '@' + $env.target_domain + ':' + $env.target_port + ';user=phone'
⊗	From	'<sip:' + $from.uri.user + '@' + $env.target_src_domain + ':' + $env.target_port + ' ;user=phone>'
⊗	To	$to.dispname + '<sip:' + $to.uri.user + '@' + $env.target_domain + ':' + $env.target_port + ';user=phone>'
⊗	Contact	'<sip:' + $from.uri.user + '@' + $env.target_src_domain + ':' + $env.out_intf_port + ';transport=TLS>' + $contact.parameter

Header: Request-URI

Add

Value:



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
☒	CUCM	✓			✓	
☒	VirginMedia	✓			✓	
☒	Anonymous	✓			✓	
☒	Noplus	✓			✓	
☒	ToTeams	✓			✓	✓
☒	FromTeams2Server	✓			✓	✓
☒	FromTeams2ServerAnonymous	✓			✓	✓
☒	999	✓			✓	
☒	112	✓			✓	
☒	18000	✓			✓	
☒	From911TeamsServer	✓			✓	✓
☒	From1TeamServer	✓			✓	✓

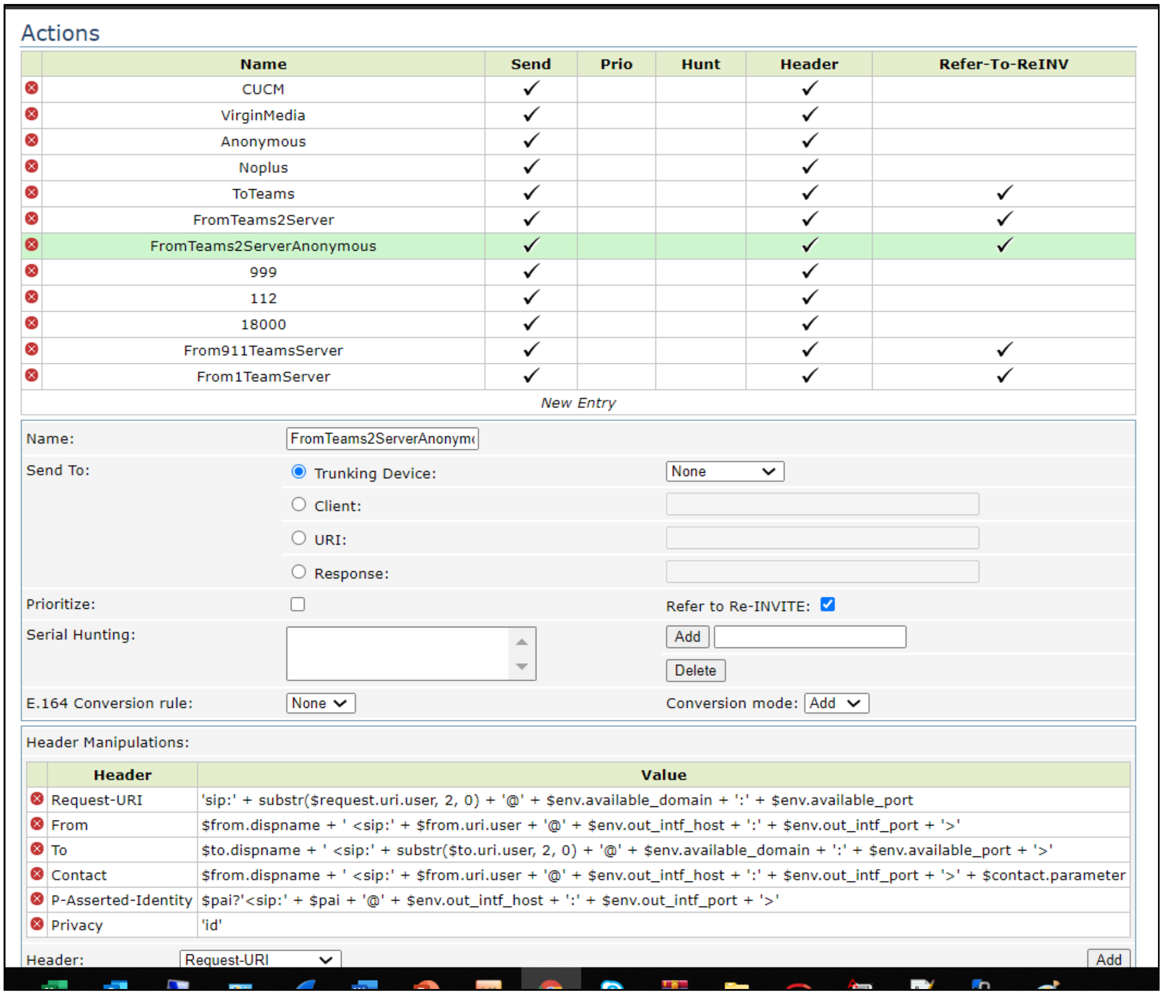
New Entry

Name:	FromTeams2Server	
Send To:	● Trunking Device:	None
	○ 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:' + $from.uri.user + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>'
☒	Contact	$from.dispname + ' <sip:' + $from.uri.user + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>' + $contact.parameter
☒	Request-URI	'sip:' + substr($request.uri.user, 2, 0) + '@' + $env.available_domain + ':' + $env.available_port
☒	To	$to.dispname + ' <sip:' + substr($to.uri.user, 2, 0) + '@' + $env.available_domain + ':' + $env.available_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'

Header: Request-URI Add



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
☒	CUCM	✓			✓	
☒	VirginMedia	✓			✓	
☒	Anonymous	✓			✓	
☒	Noplus	✓			✓	
☒	ToTeams	✓			✓	✓
☒	FromTeams2Server	✓			✓	✓
☒	FromTeams2ServerAnonymous	✓			✓	✓
☒	999	✓			✓	
☒	112	✓			✓	
☒	18000	✓			✓	
☒	From911TeamsServer	✓			✓	✓
☒	From1TeamServer	✓			✓	✓

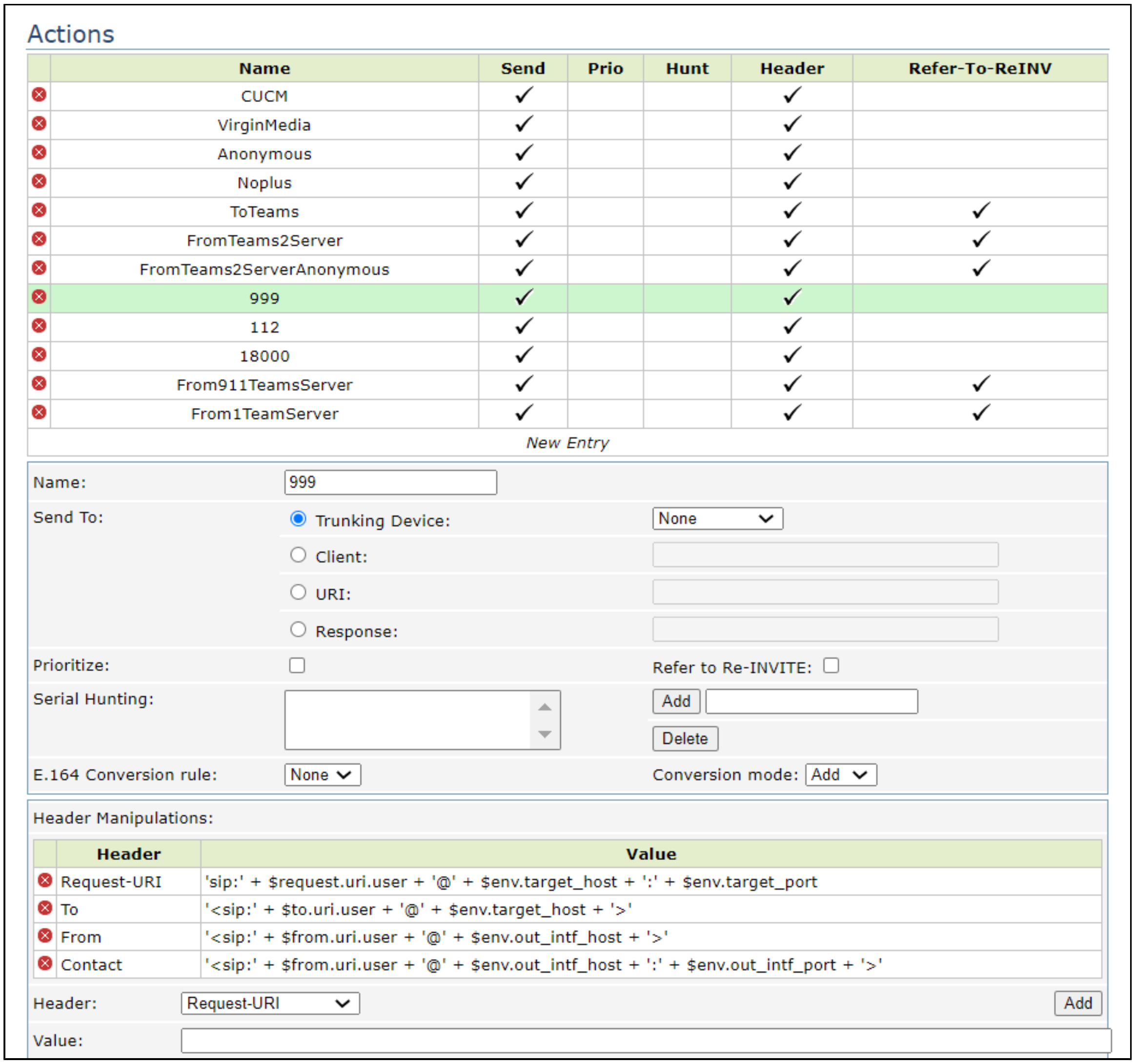
New Entry

Name:	FromTeams2ServerAnonymo	
Send To:	● Trunking Device:	None
	○ Client:	
	○ URI:	
	○ Response:	
Prioritize:	□	Refer to Re-INVITE: ☑
Serial Hunting:		Add Delete
E.164 Conversion rule:	None	Conversion mode: Add

Header Manipulations:

	Header	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:' + $pai + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>'
☒	Privacy	'id'

Header: Request-URI Add



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
⊗	CUCM	✓			✓	
⊗	VirginMedia	✓			✓	
⊗	Anonymous	✓			✓	
⊗	Noplus	✓			✓	
⊗	ToTeams	✓			✓	✓
⊗	FromTeams2Server	✓			✓	✓
⊗	FromTeams2ServerAnonymous	✓			✓	✓
⊗	999	✓			✓	
⊗	112	✓			✓	
⊗	18000	✓			✓	
⊗	From911TeamsServer	✓			✓	✓
⊗	From1TeamServer	✓			✓	✓
	New Entry					

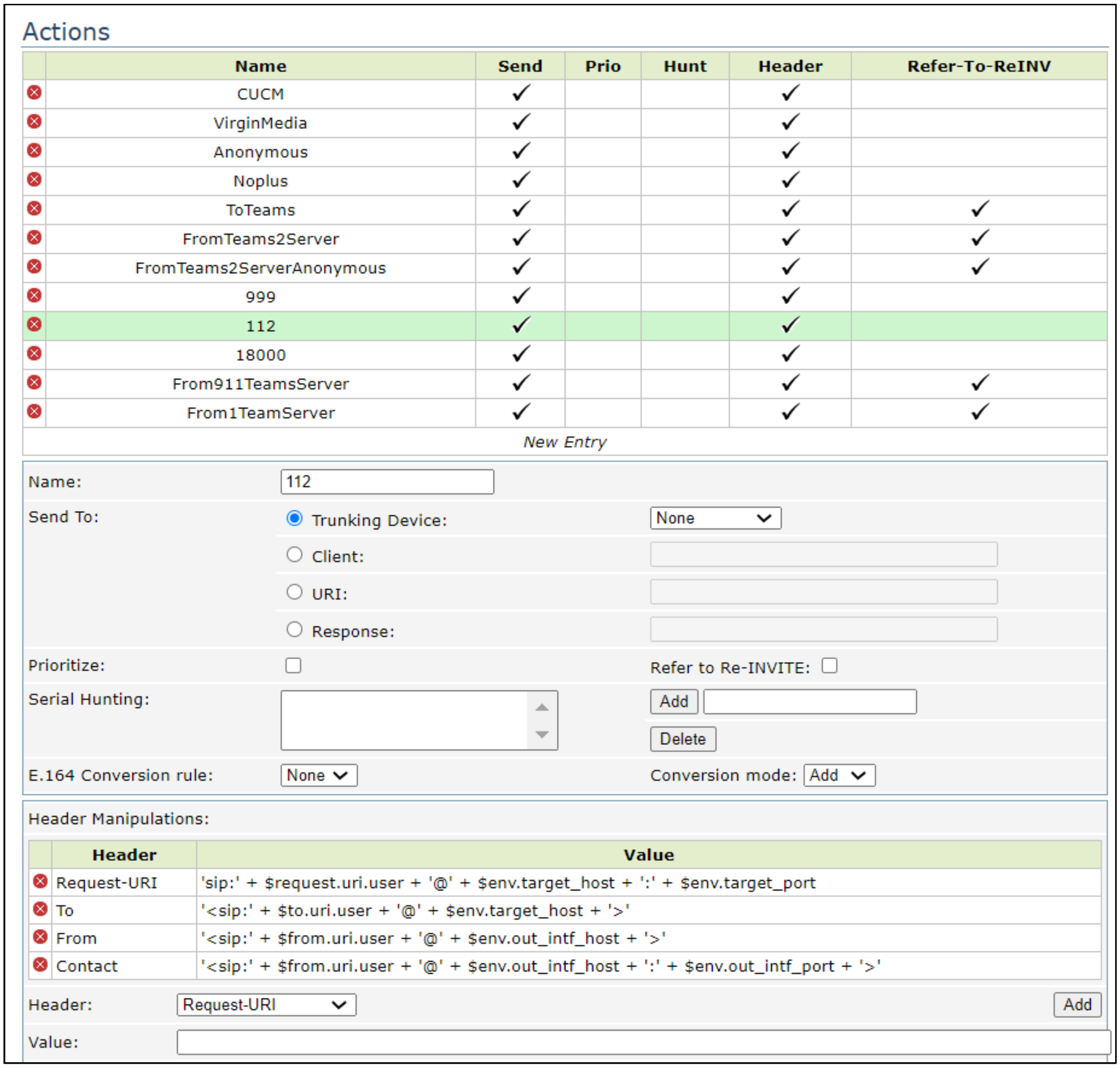
Name:	999		
Send To:	● Trunking Device:	None	
	○ Client:		
	○ URI:		
	○ Response:		
Prioritize:	□	Refer to Re-INVITE: □	
Serial Hunting:		Add	
		Delete	
E.164 Conversion rule:	None	Conversion mode: Add	

Header Manipulations:

	Header	Value
⊗	Request-URI	'sip:' + $request.uri.user + '@' + $env.target_host + ':' + $env.target_port
⊗	To	'<sip:' + $to.uri.user + '@' + $env.target_host + '>'
⊗	From	'<sip:' + $from.uri.user + '@' + $env.out_intf_host + '>'
⊗	Contact	'<sip:' + $from.uri.user + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>'

Header: Request-URI Add

Value:



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
⊗	CUCM	✓			✓	
⊗	VirginMedia	✓			✓	
⊗	Anonymous	✓			✓	
⊗	Noplus	✓			✓	
⊗	ToTeams	✓			✓	✓
⊗	FromTeams2Server	✓			✓	✓
⊗	FromTeams2ServerAnonymous	✓			✓	✓
⊗	999	✓			✓	
⊗	112	✓			✓	
⊗	18000	✓			✓	
⊗	From911TeamsServer	✓			✓	✓
⊗	From1TeamServer	✓			✓	✓

New Entry

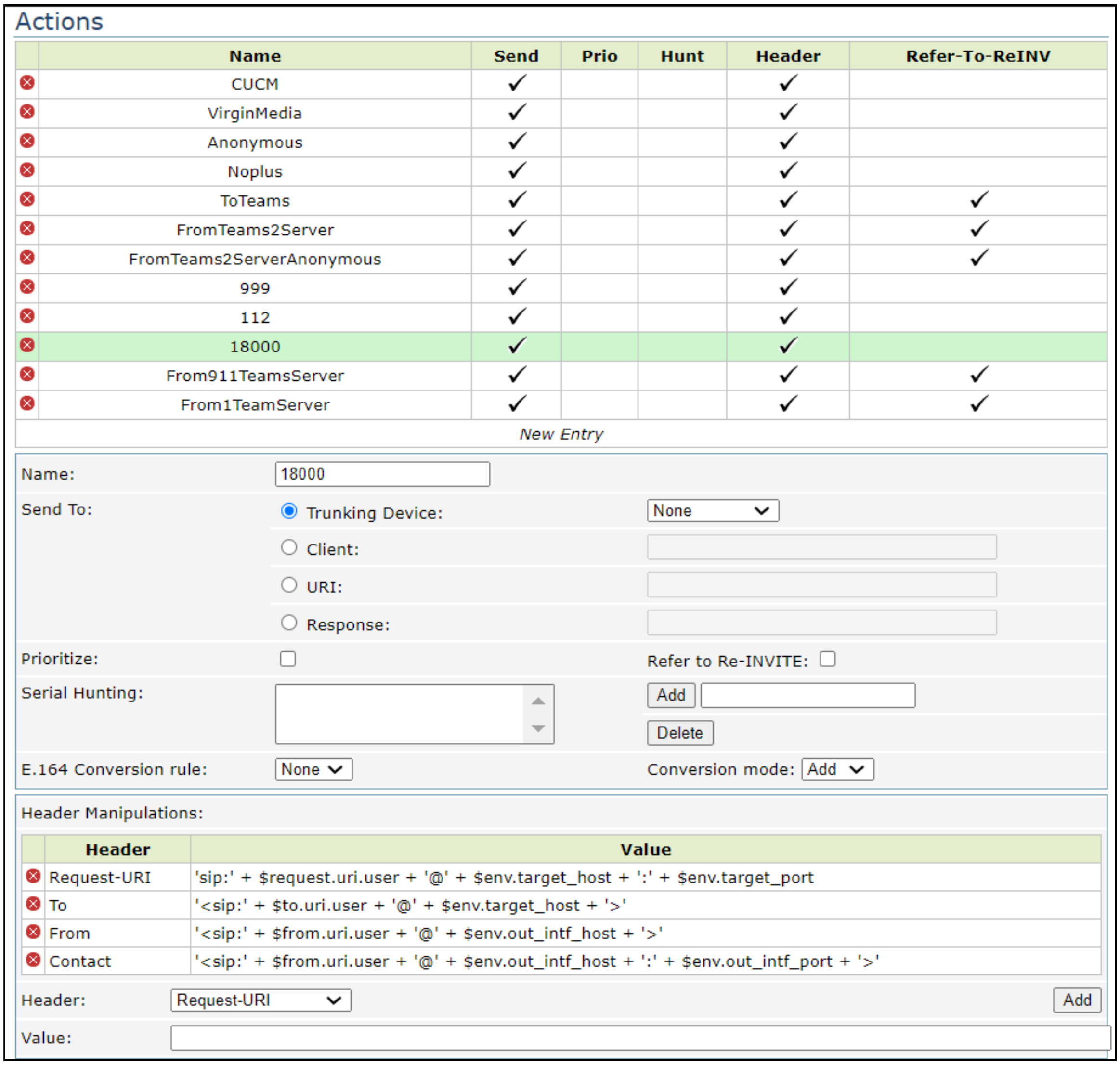
Name:	112		
Send To:	● Trunking Device:	None	
	○ Client:		
	○ URI:		
	○ Response:		
Prioritize:	□	Refer to Re-INVITE: □	
Serial Hunting:		Add	
		Delete	
E.164 Conversion rule:	None	Conversion mode: Add	

Header Manipulations:

	Header	Value
⊗	Request-URI	'sip:' + $request.uri.user + '@' + $env.target_host + ':' + $env.target_port
⊗	To	'<sip:' + $to.uri.user + '@' + $env.target_host + '>'
⊗	From	'<sip:' + $from.uri.user + '@' + $env.out_intf_host + '>'
⊗	Contact	'<sip:' + $from.uri.user + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>'

Header: Request-URI Add

Value:



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
⊗	CUCM	✓			✓	
⊗	VirginMedia	✓			✓	
⊗	Anonymous	✓			✓	
⊗	Noplus	✓			✓	
⊗	ToTeams	✓			✓	✓
⊗	FromTeams2Server	✓			✓	✓
⊗	FromTeams2ServerAnonymous	✓			✓	✓
⊗	999	✓			✓	
⊗	112	✓			✓	
⊗	18000	✓			✓	
⊗	From911TeamsServer	✓			✓	✓
⊗	From1TeamServer	✓			✓	✓

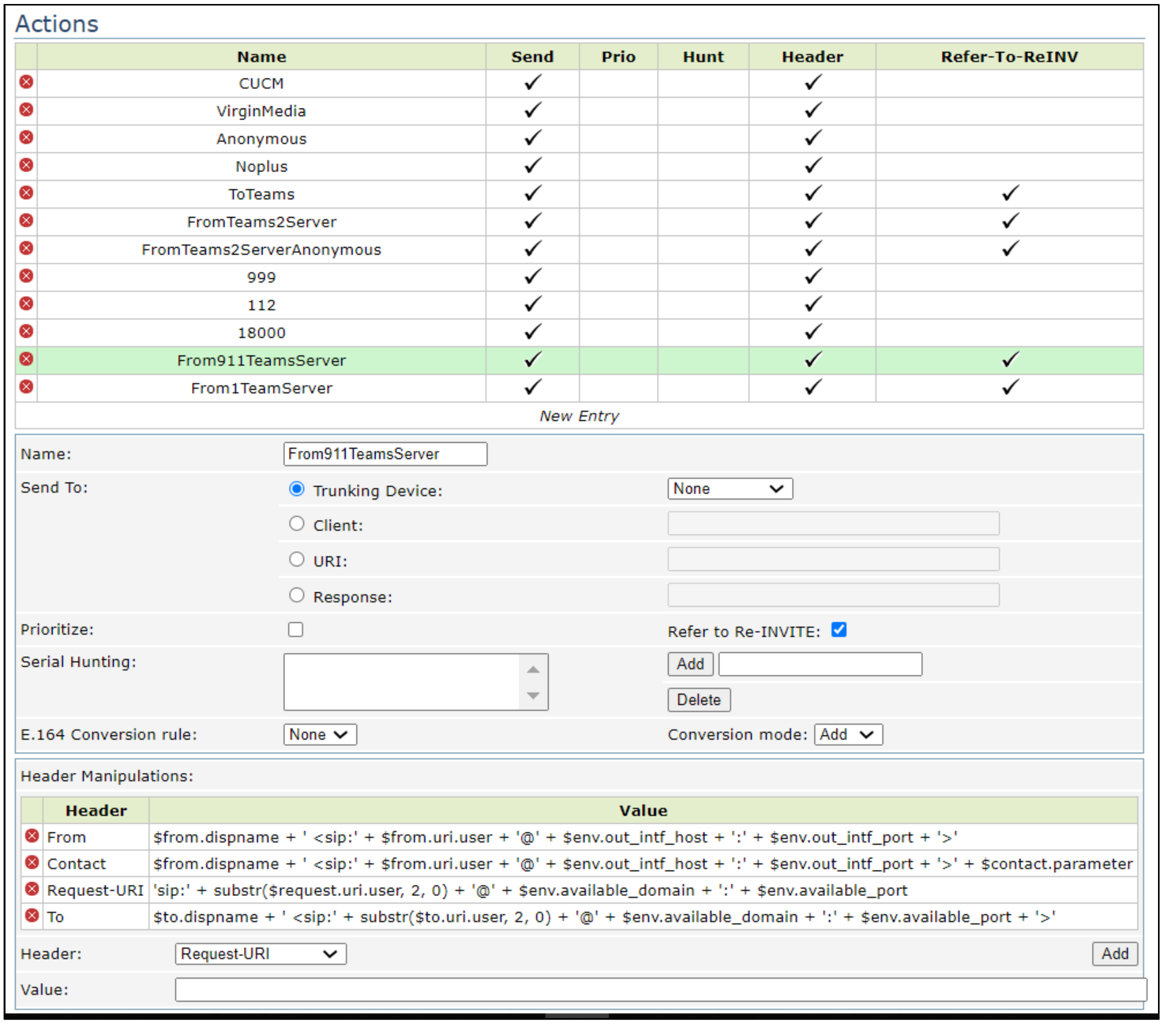
New Entry

Name:	18000		
Send To:	● Trunking Device:	None	
	○ Client:		
	○ URI:		
	○ Response:		
Prioritize:	□	Refer to Re-INVITE: □	
Serial Hunting:		Add	
		Delete	
E.164 Conversion rule:	None	Conversion mode:	Add

Header Manipulations:

	Header	Value
⊗	Request-URI	'sip:' + $request.uri.user + '@' + $env.target_host + ':' + $env.target_port
⊗	To	'<sip:' + $to.uri.user + '@' + $env.target_host + '>'
⊗	From	'<sip:' + $from.uri.user + '@' + $env.out_intf_host + '>'
⊗	Contact	'<sip:' + $from.uri.user + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>'

Header:	Request-URI	Add
Value:		



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
☒	CUCM	✓			✓	
☒	VirginMedia	✓			✓	
☒	Anonymous	✓			✓	
☒	Noplus	✓			✓	
☒	ToTeams	✓			✓	✓
☒	FromTeams2Server	✓			✓	✓
☒	FromTeams2ServerAnonymous	✓			✓	✓
☒	999	✓			✓	
☒	112	✓			✓	
☒	18000	✓			✓	
☒	From911TeamsServer	✓			✓	✓
☒	From1TeamServer	✓			✓	✓

New Entry

Name: From911TeamsServer

Send To: ● Trunking Device: None

○ Client:

○ URI:

○ Response:

Prioritize: □ Refer to Re-INVITE: ☑

Serial Hunting:

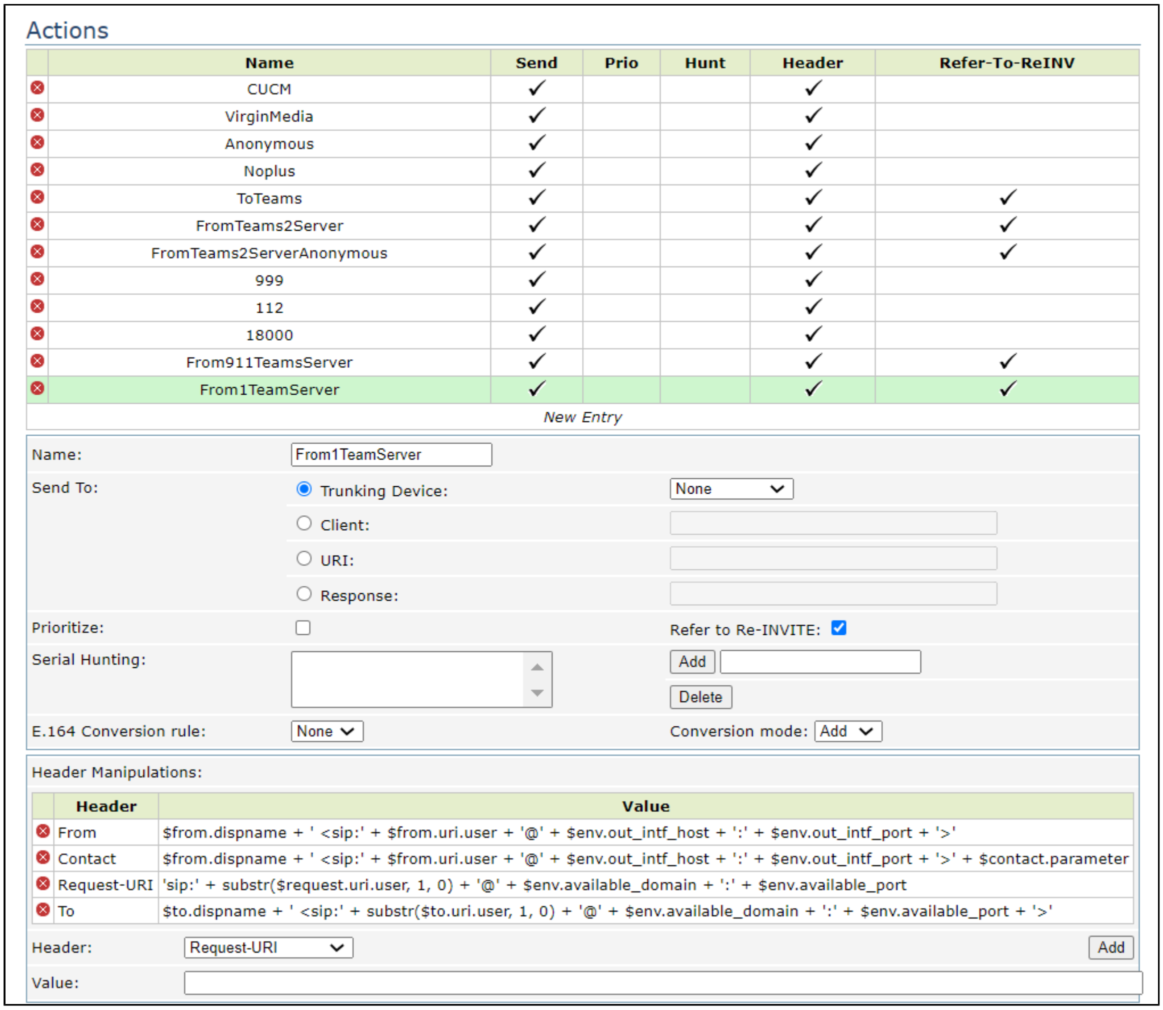
E.164 Conversion rule: None Conversion mode: Add

Header Manipulations:

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

Header: Request-URI

Value:



Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
☒	CUCM	✓			✓	
☒	VirginMedia	✓			✓	
☒	Anonymous	✓			✓	
☒	Noplus	✓			✓	
☒	ToTeams	✓			✓	✓
☒	FromTeams2Server	✓			✓	✓
☒	FromTeams2ServerAnonymous	✓			✓	✓
☒	999	✓			✓	
☒	112	✓			✓	
☒	18000	✓			✓	
☒	From911TeamsServer	✓			✓	✓
☒	From1TeamServer	✓			✓	✓

New Entry

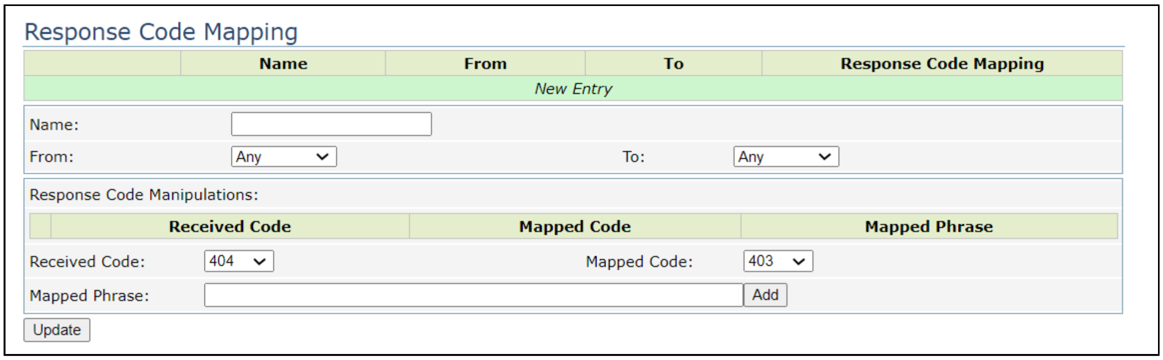
Name:	From1TeamServer	
Send To:	● Trunking Device:	None
	○ Client:	
	○ URI:	
	○ Response:	
Prioritize:	□	Refer to Re-INVITE: ☑
Serial Hunting:		Add Delete
E.164 Conversion rule:	None	Conversion mode: Add

Header Manipulations:

	Header	Value
☒	From	$from.dispname + ' <sip:' + $from.uri.user + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>'
☒	Contact	$from.dispname + ' <sip:' + $from.uri.user + '@' + $env.out_intf_host + ':' + $env.out_intf_port + '>' + $contact.parameter
☒	Request-URI	'sip:' + substr($request.uri.user, 1, 0) + '@' + $env.available_domain + ':' + $env.available_port
☒	To	$to.dispname + ' <sip:' + substr($to.uri.user, 1, 0) + '@' + $env.available_domain + ':' + $env.available_port + '>'

Header: Request-URI

Value:



Response Code Mapping

	Name	From	To	Response Code Mapping

New Entry

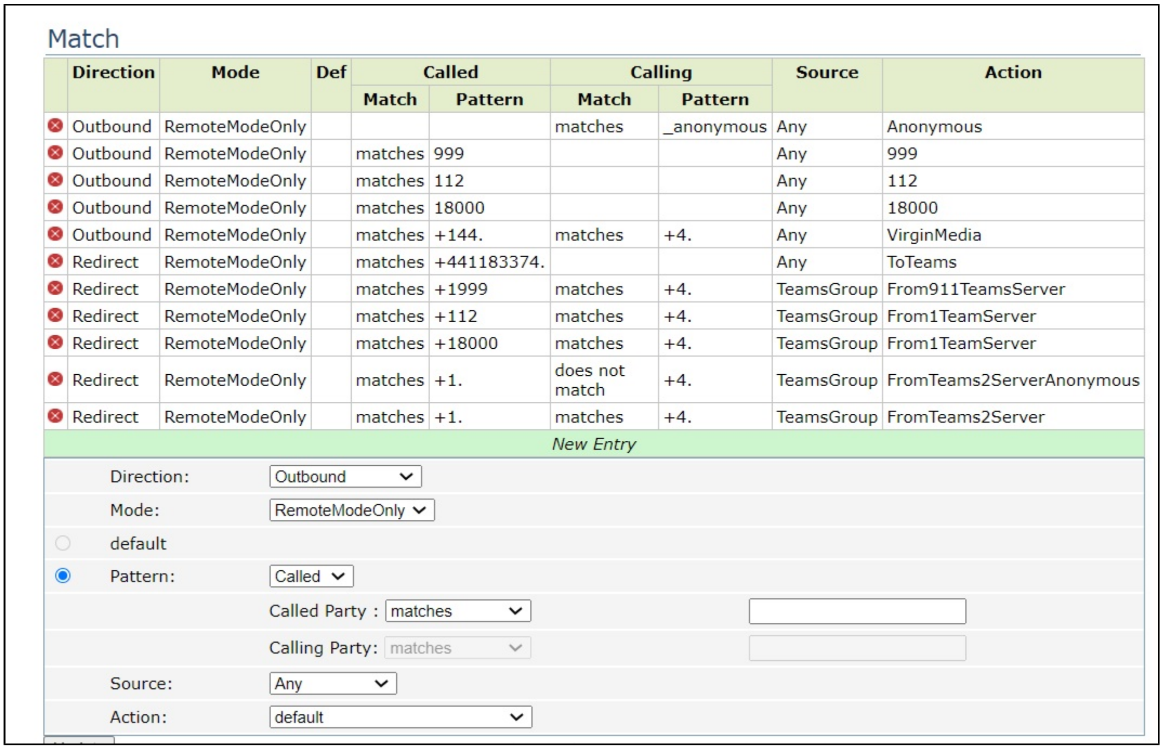
Name:			
From:	Any	To:	Any

Response Code Manipulations:

	Received Code	Mapped Code	Mapped Phrase

Received Code: 404 Mapped Code: 403

Mapped Phrase:



Match

	Direction	Mode	Def	Called		Calling		Source	Action
				Match	Pattern	Match	Pattern		
⊗	Outbound	RemoteModeOnly				matches	_anonymous	Any	Anonymous
⊗	Outbound	RemoteModeOnly		matches	999			Any	999
⊗	Outbound	RemoteModeOnly		matches	112			Any	112
⊗	Outbound	RemoteModeOnly		matches	18000			Any	18000
⊗	Outbound	RemoteModeOnly		matches	+144.	matches	+4.	Any	VirginMedia
⊗	Redirect	RemoteModeOnly		matches	+441183374.			Any	ToTeams
⊗	Redirect	RemoteModeOnly		matches	+1999	matches	+4.	TeamsGroup	From911TeamsServer
⊗	Redirect	RemoteModeOnly		matches	+112	matches	+4.	TeamsGroup	From1TeamServer
⊗	Redirect	RemoteModeOnly		matches	+18000	matches	+4.	TeamsGroup	From1TeamServer
⊗	Redirect	RemoteModeOnly		matches	+1.	does not match	+4.	TeamsGroup	FromTeams2ServerAnonymous
⊗	Redirect	RemoteModeOnly		matches	+1.	matches	+4.	TeamsGroup	FromTeams2Server

New Entry

Direction: Outbound

Mode: RemoteModeOnly

○ default

● Pattern: Called

Called Party : matches

Calling Party: matches

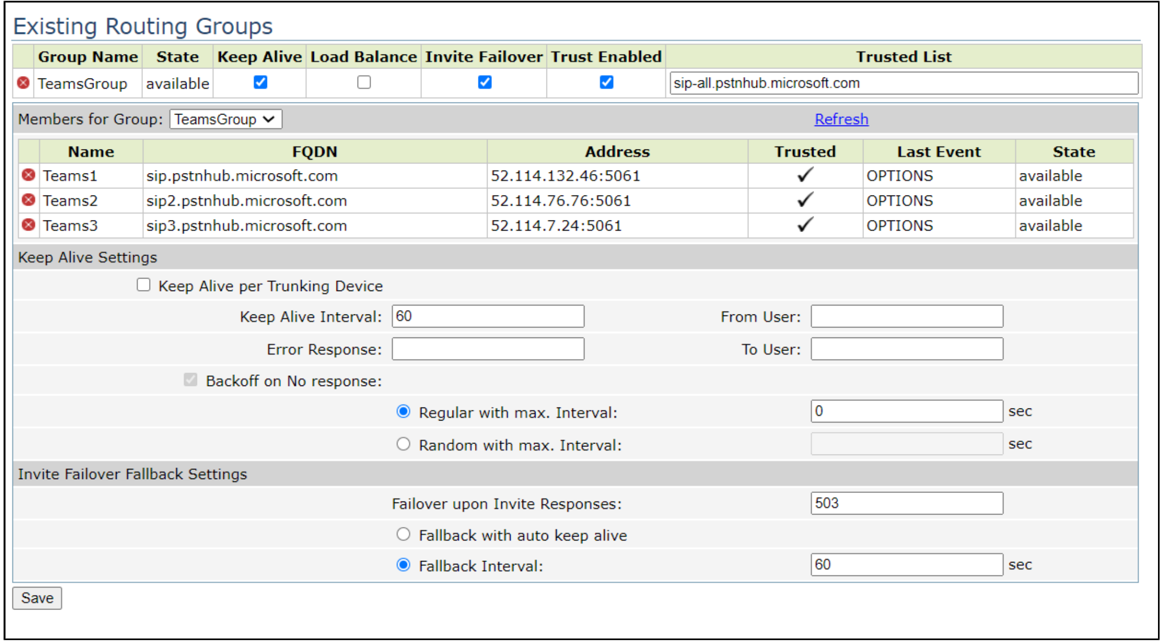
Source: Any

Action: default

Trunking Group Availability

1. Click *VoIP* > *Trunking Group Availability*.
2. Configure the Group "Teams Group" with Teams1 (sip.pstnhub.microsoft.com), Teams2 (sip2.pstnhub.microsoft.com), Teams3 (sip3.pstnhub.microsoft.com).

Figure 10: Trunking Group Availability



Existing Routing Groups

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

Members for Group: TeamsGroup Refresh

	Name	FQDN	Address	Trusted	Last Event	State
⊗	Teams1	sip.pstnhub.microsoft.com	52.114.132.46:5061	✓	OPTIONS	available
⊗	Teams2	sip2.pstnhub.microsoft.com	52.114.76.76:5061	✓	OPTIONS	available
⊗	Teams3	sip3.pstnhub.microsoft.com	52.114.7.24:5061	✓	OPTIONS	available

Keep Alive Settings

☐ Keep Alive per Trunking Device

Keep Alive Interval: 60 From User:

Error Response: To User:

☑ Backoff on No response:

● Regular with max. Interval: 0 sec

○ Random with max. Interval: sec

Invite Failover Fallback Settings

Failover upon Invite Responses: 503

○ Fallback with auto keep alive

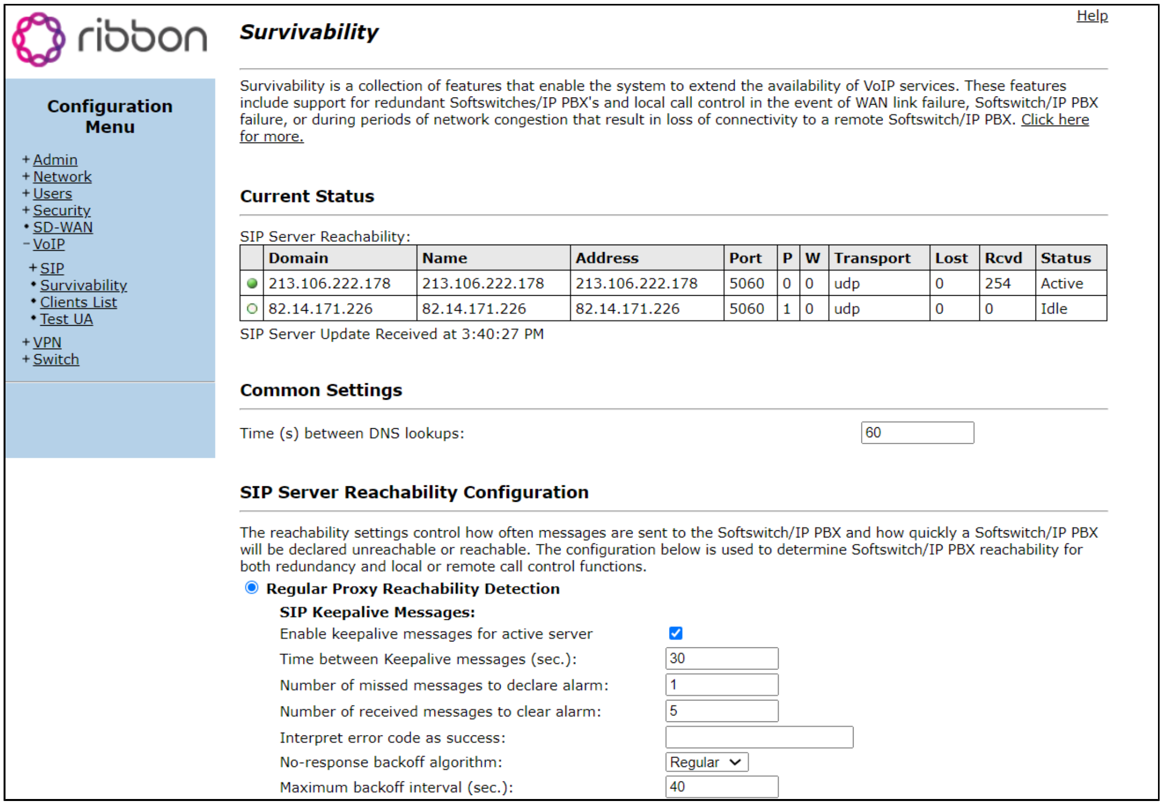
● Fallback Interval: 60 sec

Save

Survivability

1. Click *VoIP* > *Survivability.*
2. Configure the parameters.

Figure 11: Survivability



Survivability

Survivability is a collection of features that enable the system to extend the availability of VoIP services. These features include support for redundant Softswitches/IP PBX's and local call control in the event of WAN link failure, Softswitch/IP PBX failure, or during periods of network congestion that result in loss of connectivity to a remote Softswitch/IP PBX. Click here for more.

Current Status

SIP Server Reachability:

	Domain	Name	Address	Port	P	W	Transport	Lost	Rcvd	Status
●	213.106.222.178	213.106.222.178	213.106.222.178	5060	0	0	udp	0	254	Active
○	82.14.171.226	82.14.171.226	82.14.171.226	5060	1	0	udp	0	0	Idle

SIP Server Update Received at 3:40:27 PM

Common Settings

Time (s) between DNS lookups: 60

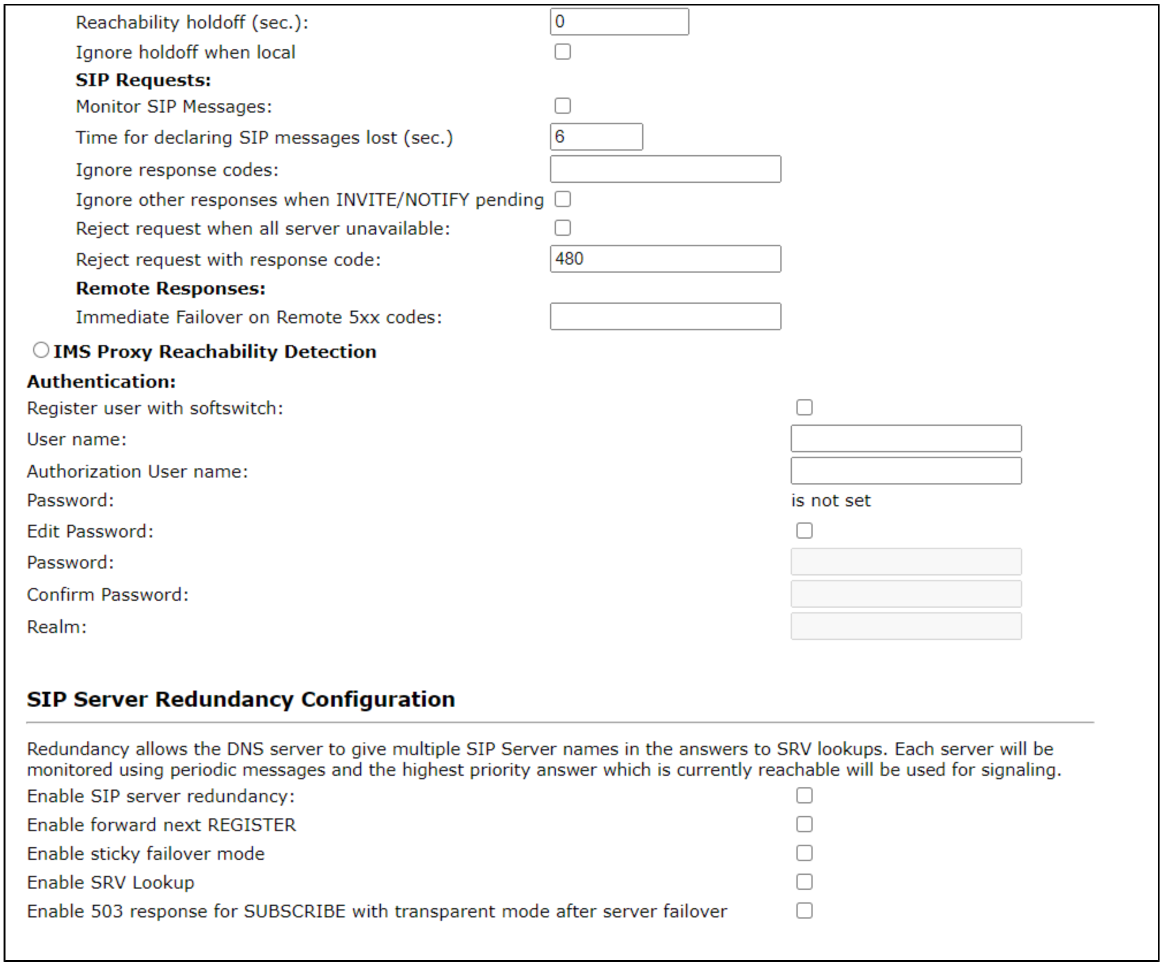
SIP Server Reachability Configuration

The reachability settings control how often messages are sent to the Softswitch/IP PBX and how quickly a Softswitch/IP PBX will be declared unreachable or reachable. The configuration below is used to determine Softswitch/IP PBX reachability for both redundancy and local or remote call control functions.

● **Regular Proxy Reachability Detection**

SIP Keepalive Messages:

Enable keepalive messages for active server	☑
Time between Keepalive messages (sec.):	30
Number of missed messages to declare alarm:	1
Number of received messages to clear alarm:	5
Interpret error code as success:	
No-response backoff algorithm:	Regular
Maximum backoff interval (sec.):	40



Reachability holdoff (sec.):	0
Ignore holdoff when local	□
SIP Requests:	
Monitor SIP Messages:	□
Time for declaring SIP messages lost (sec.)	6
Ignore response codes:	
Ignore other responses when INVITE/NOTIFY pending	□
Reject request when all server unavailable:	□
Reject request with response code:	480
Remote Responses:	
Immediate Failover on Remote 5xx codes:	

○ **IMS Proxy Reachability Detection**

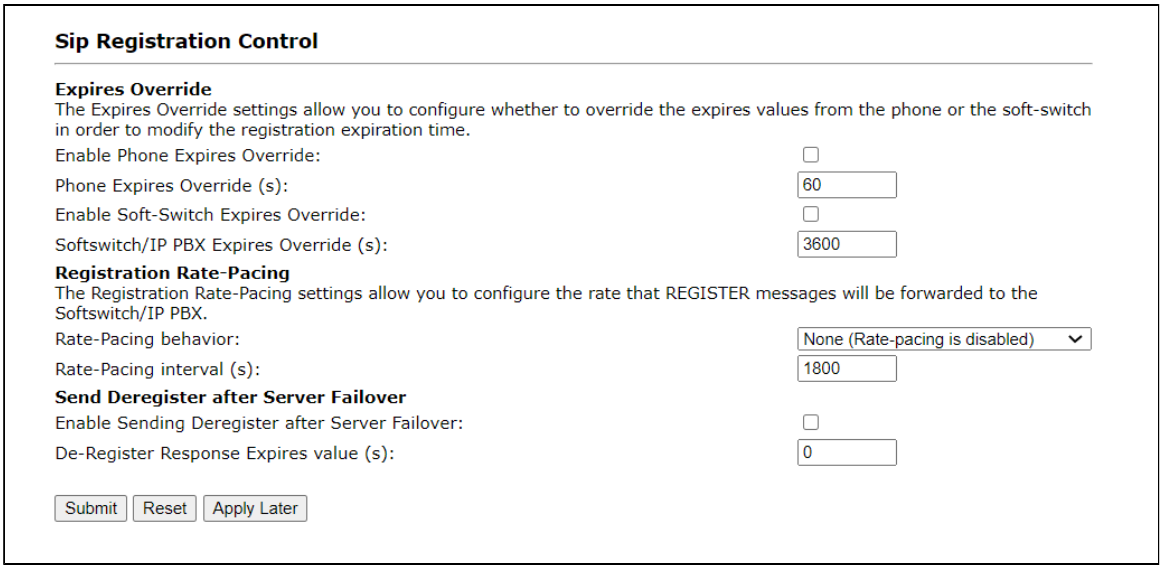
Authentication:

Register user with softswitch:	□
User name:	
Authorization User name:	
Password:	is not set
Edit Password:	□
Password:	
Confirm Password:	
Realm:	

SIP Server Redundancy Configuration

Redundancy allows the DNS server to give multiple SIP Server names in the answers to SRV lookups. Each server will be monitored using periodic messages and the highest priority answer which is currently reachable will be used for signaling.

Enable SIP server redundancy:	□
Enable forward next REGISTER	□
Enable sticky failover mode	□
Enable SRV Lookup	□
Enable 503 response for SUBSCRIBE with transparent mode after server failover	□



Sip Registration Control

Expires Override
The Expires Override settings allow you to configure whether to override the expires values from the phone or the soft-switch in order to modify the registration expiration time.

Enable Phone Expires Override:	□
Phone Expires Override (s):	60
Enable Soft-Switch Expires Override:	□
Softswitch/IP PBX Expires Override (s):	3600

Registration Rate-Pacing
The Registration Rate-Pacing settings allow you to configure the rate that REGISTER messages will be forwarded to the Softswitch/IP PBX.

Rate-Pacing behavior:	None (Rate-pacing is disabled)
Rate-Pacing interval (s):	1800

Send Deregister after Server Failover

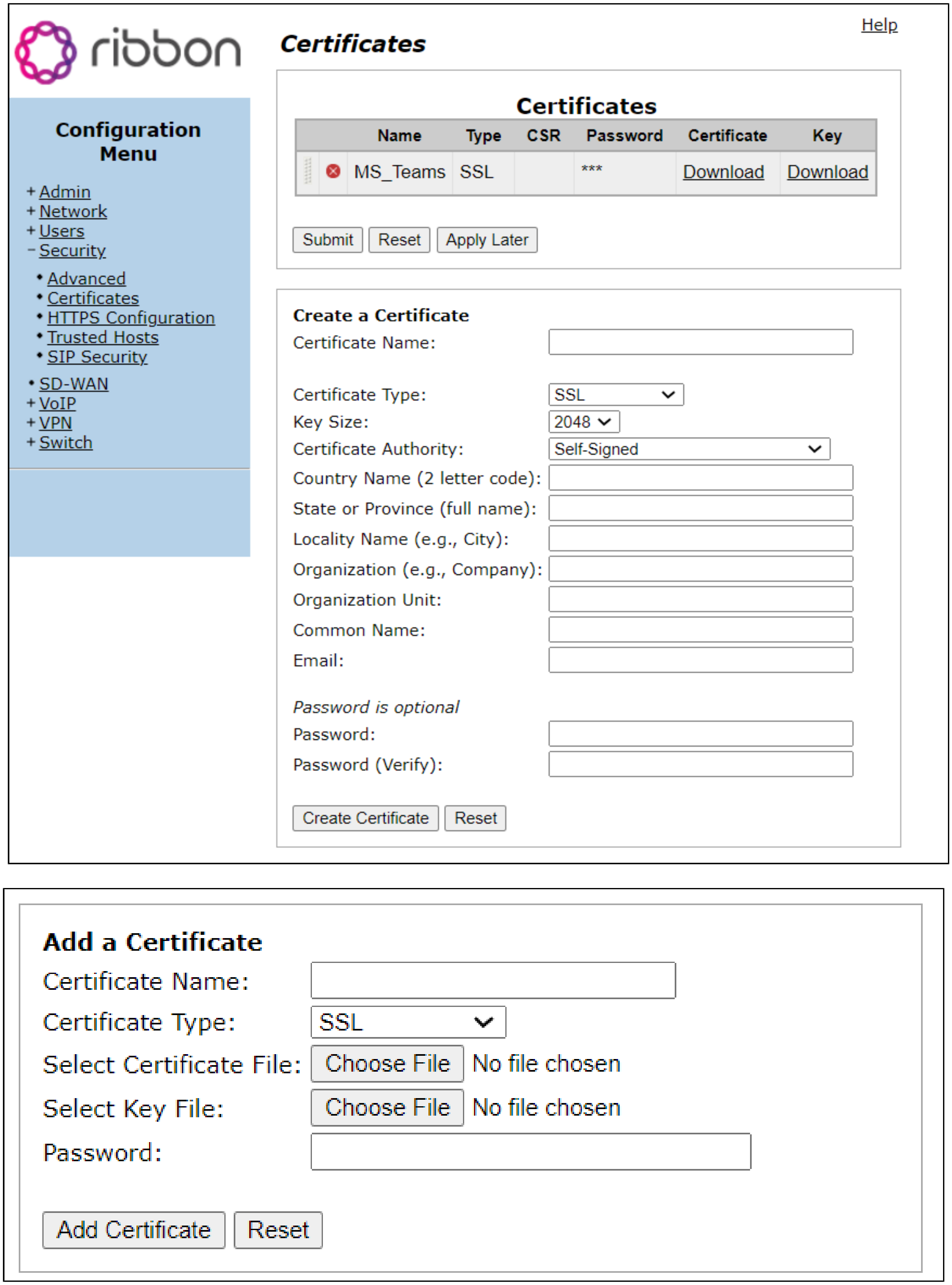
Enable Sending Deregister after Server Failover:	□
De-Register Response Expires value (s):	0

Security

Certificates

1. Click *Security* > *Certificates.*
2. Add the Certificate and upload the Certificate that you will use with MS Teams for communication.

Figure 12: Certificate



Certificates

Certificates

	Name	Type	CSR	Password	Certificate	Key
⊗	MS_Teams	SSL		***	Download	Download

Create a Certificate

Certificate Name:	
Certificate Type:	SSL
Key Size:	2048
Certificate Authority:	Self-Signed
Country Name (2 letter code):	
State or Province (full name):	
Locality Name (e.g., City):	
Organization (e.g., Company):	
Organization Unit:	
Common Name:	
Email:	

Password is optional

Password:	
Password (Verify):	

Add a Certificate

Certificate Name:	
Certificate Type:	SSL
Select Certificate File:	No file chosen
Select Key File:	No file chosen
Password:	

Test Results

The following table provides information about the tests that Ribbon performed to complete all scenarios that Virgin Media needs for its customers.

S. No	Procedure	Observation	Result	Comment
IOP1	Vendors eSBC response to SIP OPTIONS messages from SBC	No calls are required for this test. Capture the SIP trace for approximately 60 seconds and check for correct signaling. For each eSBC, the SBC periodically sends an OPTIONS request to the vendors eSBC to check if its SIP stack is reachable. If the IP-PBX sends a SIP response 200 OK, the SIP trunk is placed or remains in an In-Service state. **Example:** OPTIONS sip:ping@<ip-pbx_IP_Addr>:5060 SIP/2.0	Pass	
IOP2	SBC response to SIP OPTIONS messages from vendor eSBC	No calls are required for this test. Capture SIP trace for approximately 60 seconds (depending on agreement) and check for correct signaling. **Vendors eSBC setup for Solution IP.Addr Mode** • The eSBC is configured to send OPTIONS messages to the SBC periodically. • The SBC responds with SIP response 200 OK. **Example:** "OPTIONS sip:ping@192.168.1.10:5060 SIP/2.0" • Verify that the eSBC can simultaneously send SIP OPTIONS messages to both the solution SBC addresses.	Pass	
IOP4	Basic test call from IP-PBX to PSTN line through SBC-A (using SBC-A IPV4 ip address)	• The IP-PBX line initiates the call. • The call is answered. • The IP-PBX line terminates the call. **Vendors eSBC setup for Solution IP.Addr Mode** A call progresses successfully when: • A call is received from the IP-PBX. • An Invite is seen from the eSBC to SBC-A. • Proxy authentication challenge is returned to the eSBC. • A Re-invite with correct credentials is received from the eSBC. **Example:** Request-Line: INVITE sip:<B-party>@<SBC-A ip.addr TBD>: 5060 SIP/2.0 To: sip:<B-Party>@<SBC-A ip.addr TBD> • Check the Wireshark trace to confirm that the G.711 A law codec with 10 or 20ms packetization is used. • Verify that the INVITE contains the Session-Expires header, and the INVITE is syntactically correct. • Check the Supported Header to ensure that it supports the 'timer'. Ensure that the response in the 200 OK is compatible with the INVITE. Also, verify that the Required Header contains the 'timer'.	Pass	

IOP5	Basic test call from IP-PBX to PSTN line through SBC-B (using SBC-B IPV4 ip address) Vendor to configure eSBC so that it used secondary SBC (SBC_B) for this test Once the test completes, eSBC to be configured to use Primary SBC-A for calls to route to	• The IP-PBX line initiates the call. • The call is answered. • The IP-PBX line terminates the call. **Vendors eSBC setup for Solution IP.Addr Mode** A call progresses successfully when: • A call is received from the IP-PBX. • An Invite is seen from the eSBC to SBC-B. • Proxy authentication challenge is returned to the eSBC. • A re-invite with correct credentials is received from the eSBC. **Example:** Request-Line: INVITE sip:<B-party>@<SBC-B ip.addr TBD>: 5060 SIP/2.0 To: sip:<B-Party>@<SBC-B ip.addr TBD> Check the Wireshark trace to confirm that the G.711 A law codec with 10ms or 20ms packetization is used.	Pass	
IOP7b	Called Number format - vendors eSBC to soft switch number normalization - Global Dial Plan Test eSBC capability to send the called number in one of the following Global number formats (user part of Request & To URIs) 0yyyyyyyyyy (where y refers to any number, calling party = national) +44yyyyyyyyyy (where y refers to any number, calling party = national) +yyyyyyyyyy (where y refers to any number, calling party = international) yyyyyyyyyy (where y refers to any number, calling party = unknown)	Configure the SBC for Global calling plan. • The IP-PBX line initiates a call to the PSTN line. • The call is answered. • The IP-PBX line terminates the call. • Configure the eSBC to present the called number in the user part of the **Request & To URIs** and send it in one of the following formats: • 0yyyyyyyyyy (where y refers to any number, calling party = national) • +44yyyyyyyyyy (where y refers to any number, calling party = national) • +yyyyyyyyyy (where y refers to any number, calling party = international) • yyyyyyyyyy (where y refers to any number, calling party = unknown)	Pass	
IOP8b	Calling Number format - vendors eSBC to soft switch number normalization - Global Dial Plan Test eSBC capability to send calling number in one of the following Global number formats (user part of FROM & PAI URIs) 0yyyyyyyyyy (where y refers to any number, calling party = national) +44yyyyyyyyyy (where y refers to any number, calling party = national) 00yyyyyyyyyy (where y refers to any number, calling party = international) yyyyyyyyyy (where y refers to any number, calling party = unknown)	Configure the SBC for Global calling plan. • The IP-PBX line initiates a call to the PSTN line. • The call is answered. • The IP-PBX terminates the call. • Configure the eSBC to present the calling number in the user part of the **From & PAI URIs** and send it in one of the following formats: • 0yyyyyyyyyy (where y refers to any number, calling party = national) • +44yyyyyyyyyy (where y refers to any number, calling party = national) • 00yyyyyyyyyy (where y refers to any number, calling party = international) • yyyyyyyyyy (where y refers to any number, calling party = unknown)	Pass	

IOP9b	Called Number format - soft switch to eSBC number normalization - Global Dial Plan Test eSBC capability of accepting the called number in one of the following Global number formats (user part of Request & To URIs) +44yyyyyyyyy (where y refers to any number, calling party = national) +yyyyyyyyy (where y refers to any number, calling party = international) yyyyyyyyyy (where y refers to any number, calling party = unknown)	Configure the SBC for Global calling plan. • The PSTN line initiates a call to the IP-PBX line. • The call is answered. • The PSTN line terminates the call. • Configure the eSBC to accept the called number in the user part of the **Request & To URIs** in one of the following formats: • +44yyyyyyyyy (where y refers to any number, calling party = national) • +yyyyyyyyy (where y refers to any number, calling party = international) • yyyyyyyyyy (where y refers to any number, calling party = unknown) • Verify that the INVITE contains the Session-Expires header and the INVITE is syntactically correct. • Check the Supported Header to ensure that it supports the 'timer'. Ensure that the response in the 200 OK is compatible with the INVITE. Also, verify that the Required Header contains the 'timer'.	Pass	
IOP10b	Calling Number format - soft switch to eSBC number normalization - Global Dial Plan Test eSBC capability of accepting the calling number in one of the following Global number formats (user part of FROM & PAI URIs) +44yyyyyyyyy (where y refers to any number, calling party = national) +yyyyyyyyy (where y refers to any number, calling party = international) yyyyyyyyyy (where y refers to any number, calling party = unknown)	Configure the SBC for Global calling plan. • The PSTN line initiates a call to the IP-PBX line. • The call is answered. • The PSTN line terminates the call. • Configure the eSBC to accept the calling number in the user part of the **Request & To URIs** in one of the following formats: • +44yyyyyyyyy (where y refers to any number, calling party = national) • +yyyyyyyyy (where y refers to any number, calling party = international) • yyyyyyyyyy (where y refers to any number, calling party = unknown)	Pass	
IOP11	Emergency Call Handling -IP-PBX Line to PSTN - UK Emergency call 999	• Make a call from the IP-PBX line to the Emergency services using 999. • The call is answered. • Either party terminates the call. **Example:** Request-Line: INVITE sip:999@<SBC-A ip.addr TBD>:5060 SIP/2.0 To: <sip:999@<SBC-A ip.addr TBD>> From: <sip:<A-party>@<IP-PBX IP.Addr>	Pass	
IOP12	Emergency Call Handling -IP-PBX Line to PSTN - UK Emergency call 112	• Make a call from the IP-PBX line to the Emergency services using 112. • The call is answered. • Either party terminates the call. **Example:** Request-Line: INVITE sip:112@<SBC-A ip.addr TBD>:5060 SIP/2.0 To: <sip:112@<SBC-A ip.addr TBD>> From: <sip:<A-party>@<IP-PBX IP.Addr>	Pass	
IOP13	Emergency Call Handling -IP-PBX Line to PSTN - UK Emergency call 18000 - Text Direct	• Make a call from the IP-PBX line using a text direct set to the Emergency services using 18000. • The call is answered. • Either party terminates the call. **Example:** Request-Line: INVITE sip:18000@<SBC-A ip.addr TBD>:5060 SIP/2.0 To: <sip:18000@<SBC-A ip.addr TBD>> From: <sip:<A-party>@<IP-PBX IP.Addr>	Pass	

IOP14	IP-PBX Line to PSTN - call answer - Originator disconnect	• Make a call from the IP-PBX line to the PSTN line. • Answer the call. • The IP-PBX line terminates the call.	Pass	
IOP15	PSTN calls SIP #1, SIP #1 conferences in SIP #2	• Make a call from the IP-PBX line to the PSTN line. • Answer the call. • The PSTN line terminates the call.	Pass	
IOP16	IP-PBX Line to PSTN - Busy subscriber	• Make a call from the IP-PBX line to a busy PSTN line (without divert on busy). • Wait for the soft switch to return the busy response. • Ensure that the eSBC is not recursive. • Set up the call via the secondary SIP trunk.	Pass	
IOP17	IP-PBX Line to PSTN - No answer timeout test	• Make a call from the IP-PBX line to a PSTN line (without divert on no answer). • Do not answer the call. • Wait for the soft switch to return the no answer timeout response. • Ensure that the eSBC is not recursive. • Set up the call via the secondary SIP trunk.	Pass With Caveat	The timeout should be coming from our end, but 90 seconds timeout from MS Teams precedes that.
IOP18	IP-PBX Line to PSTN - Subscriber not reachable Vendor to call 01189111111	• Make a call from the IP-PBX line to an invalid number. • Wait for the soft switch to return a response. • Ensure that the eSBC is not recursive. • Set up the call via the secondary SIP trunk.	Pass	
IOP19	PSTN Line to IP-PBX - call answer - Originator disconnect.	• Make a call from a PSTN line to an IP-PBX line. • Answer the call. • The originator disconnects the call.	Pass	.
IOP20	PSTN Line to IP-PBX - call answer - Terminator disconnect	• Make a call from a PSTN line to an IP-PBX line. • Answer the call. • The IP-PBX line terminates call.	Pass	
IOP21	PSTN Line to IP-PBX - busy subscriber	• Make a call from a PSTN line to a busy IP-PBX line (without divert on busy). • Wait for the IP-PBX to return the busy response.	Not-executed	SBC team from VM advised to change this to not executed because it would mean a change to MS team server from it default configuration to get busy and we should not be change the default configuration on MS team server.
IOP22	PSTN Line to IP-PBX - No answer timeout test, Invoked by PBX	• Make a call from a PSTN line to an IP-PBX line (without divert on no answer). • Wait for the IP-PBX to return the no answer timeout response.	Pass	
IOP23	PSTN Line to IP-PBX - subscriber not reachable	• Make a call from a PSTN line to an invalid number/unprogrammed DDI on the IP-PBX. • Wait for the IP-PBX to return a response.	Pass	
IOP24	Verify CLIP service on IP-PBX line (incoming call from PSTN)	• Make a call from the PSTN line to the IP-PBX line. • The PSTN line is set to allow the CLI presentation. Check that the CLI is delivered as expected. • Either party terminates call.	Pass	

IOP25	Verify CLIR service on IP-PBX line (incoming call from PSTN)	• Make a call from the PSTN line to the IP-PBX line. • PSTN line is set to restrict the CLI presentation. Check that CLI is not delivered as expected. • Either party terminates call.	Pass	
IOP26	Verify CLIP service on PSTN line (outgoing call from IP-PBX, From)	• Ensure the number used in From header is agreed with the Virgin Media and entered into the soft switch database for screening. • Make a call from an IP-PBX line to a PSTN line. • Ensure the eSBC configuration enables the IP-PBX line to send the From header containing the Calling Line ID (CLI) in the INVITE. • Ensure that the eSBC allows the presentation of its CLI, using the privacy-header (Privacy: none or privacy-header not present). • Ensure that the expected CLI is presented to the PSTN line. • Either party terminates call.	Pass	
IOP27	Verify CLIP service on PSTN line (outgoing call from IP-PBX, PAI/PPI) Vendor to ensure PAI number is different to that from which the call originates	• Ensure the number used in the PAI/PPI header is agreed with the Virgin Media and entered into the soft switch database for screening. • Make a call from an IP-PBX line to a PSTN line. • Ensure that the eSBC configuration enables the IP-PBX line to send the PAI/PPI header containing the Calling Line ID (CLI) in the INVITE. Note that if the PAI header is populated, it will be used in preference to the From header. • Ensure that the eSBC allows the presentation of its CLI, using the privacy-header (Privacy: none or privacy-header not present). • Ensure that the expected CLI is presented to the PSTN line. • Either party terminates call.	Pass	
IOP28	Verify CLIR service on PSTN line (outgoing call from IP-PBX)	• Ensure the number used in the From/PAI header is agreed with the Virgin Media and entered into the soft switch database for screening. • Make a call from an IP-PBX line to a PSTN line. • Ensure that the eSBC configuration enables the IP-PBX line to send the From and/or PAI header, containing either the Calling Line ID or obscured information in the INVITE. **Example:** From: "user751000" <sip:+441256751000@192.168.1.10>;tag=12345 From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=12345 • Ensure that the eSBC restricts the presentation of its CLI, using the privacy-header (Privacy: id or Privacy: user or Privacy: user;id). • Ensure that CLI is NOT presented to the PSTN line. • Either party terminates call.	Pass	

IOP29	Verify Call Forward Immediate (unconditional) on a IP-PBX line (Incoming call from PSTN, call forward terminates within IP-PBX)	• Make a call from a PSTN line to an IP-PBX line with Call Forward to a line within the same IP-PBX. • Answer the call. • Either party terminates call. The IP-PBX does not have configuration settings to send SIP status 181 messages to the soft switch.	Pass	
IOP30	Verify Call Forward Immediate (unconditional) on a IP-PBX line (Incoming call from PSTN, call forward terminates PSTN)	• Make a call from a PSTN line to an IP-PBX line with Call Forward to a line in the PSTN. • Answer the call. • Either party terminates call.	Pass	
IOP31	Verify Call Forward Busy on IP-PBX line (Incoming call from PSTN, call forward terminates within IP-PBX)	• Make a call from a PSTN line to an IP-PBX line with Call Forward Busy (or equivalent) to a line within the IP-PBX. • Answer the call. • Either party terminates call.	Pass	
IOP32	Verify Call Forward No-answer on IP-PBX line (Incoming call from PSTN, call forward terminates within IP-PBX)	• Make a call from a PSTN line to an IP-PBX line with Call Forward No-answer (or equivalent) to a line within the IP-PBX. • Answer the call. • Either party terminates call.	Pass	
IOP33	Verify Call Hold Service on IP-PBX (Incoming call from PSTN)	• Make a call from a PSTN line to an IP-PBX line with Call Hold. • Answer the call. • IP-PBX line places the call on hold. • Leave the call on hold for 30 seconds and then retrieve call. • Ensure speech path is re-established in both directions. • Either party terminates call.	Pass	
IOP34	Verify 3-party conference service on IP-PBX (Incoming call from PSTN, 3rd party within IP-PBX)	• Make a call from a PSTN line to an IP-PBX line with a 3-party conference. • Answer the call. • IP-PBX line uses the 3-party conference facility to place the PSTN line on hold while dialing the 3rd party (on another IP-PBX line). • Once the 3rd party answers the call, place the 3 parties in a conference. • Ensure that all parties have a two-way speech path. Keep the speech path open for at least 20 seconds. • Either party terminates call.	Pass	
IOP35	Verify 3-party conference service on IP-PBX (Incoming call from PSTN, 3rd party PSTN)	• Make a call from a PSTN line to an IP-PBX line with a 3-party conference. • Answer the call. • IP-PBX line uses the 3-party conference facility to place the PSTN line on hold while dialing the 3rd party (on another IP-PBX line). • Once the 3rd party has answered the call, place the 3 parties in a conference. • Ensure that all parties have a two-way speech path. Keep the speech path open for at least 20 seconds. • Either party terminates call.	Pass	

IOP36	Verify do-not-disturb service on IP-PBX line (Incoming call from PSTN)	• The call does not ring. • PSTN line receives an appropriate announcement or tone. • Record the SIP status received from the IP-PBX.	Pass	
IOP37	Verify Call park service on IP-PBX line (Incoming call from PSTN)	• Make a call from a PSTN line to IP-PBX line A with Call Park (or equivalent) feature active. • Answer the call. • Place the call in the Park condition. • After 10 seconds, retrieve the call from the IP-PBX line B, using the Call Park pick-up code. • Ensure the speech path is re-established in both directions. • Either party terminates call.	Pass	
IOP38	Verify Call Waiting on an IP-PBX line, involving a PSTN line	• Make a call from PSTN line A to an IP-PBX line with Call Waiting active. • Answer the call. • Make a call from the PSTN line B to the same IP-PBX line, which should receive an indication that a second call is waiting. • PSTN line B receives the ringback tone. • IP-PBX line answers the call from the PSTN line B. • PSTN line A should receive an appropriate indication that they are now on hold. • IP-PBX line toggles the call back to PSTN line A. • Ensure the speech path is re-established in both directions and that PSTN line B receives an appropriate indication that they are now on hold. • Either party terminates call.	Pass	
IOP39	Verify DTMF transmission from/to IP-PBX - Inband	• Configure the IP-PBX/eSBC to send the DTMF transmission in-band. • Make a call from IP-PBX line to a PSTN line. • Answer the call. • PSTN line presses each of the keys on the number pad in turn. Note the far-end experience. • IP-PBX line presses each of the keys on the number pad in turn. Note the far-end experience. The received DTMF tone is reflective of the length of time the key was pressed.	Not-executed	SBC team from VM changed this to not executed as IN Band DTMF tones is not currently support and it will require a feature to be added to the code.
IOP40	Verify DTMF transmission from/to IP-PBX - RFC 2833 - telephone-event	• Configure the IP-PBX/eSBC to send the DTMF transmission, using RFC 2833 - telephone-event. • Make a call from IP-PBX line to a PSTN line. • Answer the call. • PSTN line presses each of the keys on the number pad in turn. Note the far-end experience. • IP-PBX line presses each of the keys on the number pad in turn. Note the far-end experience. The received DTMF tone is reflective the length of time the key was pressed.	Pass	

IOP41	T.38 Fax transmission mode - PSTN to IP-PBX origination	• Configure the ATA/IP-PBX/eSBC, so that the Fax transmission is sent using the T.38 Version 0 Fax transmission mode. • Make a call from PSTN line to an IP-PBX line. • Answer the call. • Fax transmission is completed, and the call is terminated by either of the end terminal devices. • Ensure the Wireshark trace shows it is using the T.38 Fax Transmission. Check that the fax is transmitted and received as expected.	Not-executed	MS Teams does not support Fax.
IOP42	T.38 Fax transmission mode - IP-PBX to PSTN origination	• Configure the ATA/IP-PBX/eSBC, so that the Fax transmission is sent using the T.38 Version 0 Fax transmission mode. • Make a call from IP-PBX line to a PSTN line. • Answer the call. • Fax transmission is completed, and the call is terminated by either of the end terminal devices. • Ensure Wireshark trace shows that the T.38 Fax Transmission is used. • Check that the fax is transmitted and received as expected.	Not-executed	MS Teams does not support Fax.
IOP43	In-band G.711 Fax transmission mode - PSTN to IP-PBX origination	• Configure the ATA/IP-PBX/eSBC, so that Fax transmission is sent using the in-band G.711 Fax transmission mode. • Make a call from the PSTN line to an IP-PBX line. • Answer the call. • Fax transmission is completed, and the call is terminated by either of the end terminal devices. • Ensure the Wireshark trace shows that the in-band G.711 Fax Transmission is used. • Check that the fax is transmitted and received as expected.	Not-executed	MS Teams does not support Fax.
IOP44	In-band G.711 Fax transmission mode - IP-PBX to PSTN origination	• Configure the ATA/IP-PBX/eSBC, so that the Fax transmission is sent using the in-band G.711 Fax transmission mode. • Make a call from IP-PBX line to a PSTN line. • Answer the call. • Fax transmission is completed, and the call is terminated by either of the end terminal devices. • Ensure the Wireshark trace shows that the in-band G.711 Fax Transmission is used. • Check that the fax is transmitted and received as expected.	Not-executed	MS Teams does not support Fax.

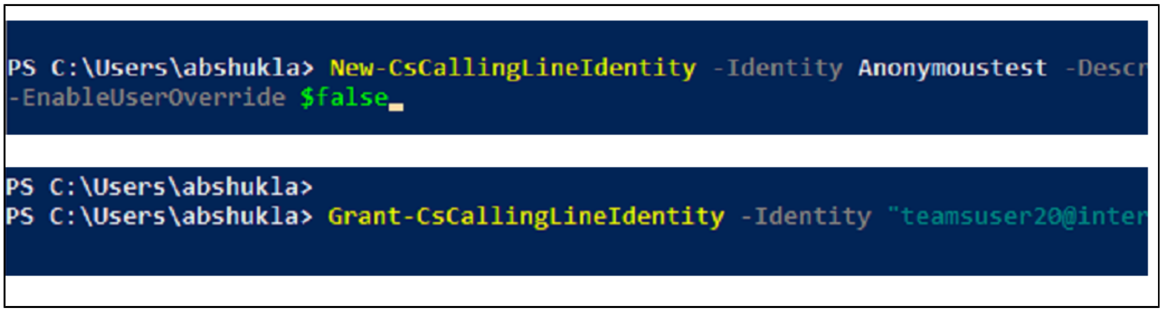
IOP45	Test for call in progress audit function (response to in-call OPTIONS from soft switch to eSBC) & session refresh & response to UPDATE messages.	• Make a call from an IP-PBX line to a PSTN line. • Answer the call. • Leave the two parties in conversation for 35 minutes. • Ensure the Session-expires setting is 3600 or less. • Ensure both parties have two-way speech at the beginning and end of call. • Either party terminates the call. • Check the Wireshark trace to ensure that the in-call OPTIONS are sent by the soft switch, and that the eSBC responds with status 200OK. • Check if the eSBC sends any in-call audit SIP messages. • Check for session refresh Update or Re-Invite and correct response.	Pass	
IOP46	Test for 4 simultaneous calls: 2 inbound, 2 outbound calls Vendor to configure eSBC for Round robin to ensure calls go to both Primary and secondary SBC	• Configure the eSBC, so that successive calls route to alternate SBCs (round robin, cyclic, and so on). • Make 4 simultaneous calls: 2 inbound and 2 outbound calls. • Answer the calls and ensure two-way speech path for each call.	Not-executed	Round robin outbound calls is not a feature of the EdgeMarc platform. Adding this feature requires a change in the Edgemarc code.
IOP47	Test for eSBC endpoint restart-recovery	• Restart the eSBC. • Ensure that, after recovery, inbound and outbound calls are successful.	Pass	
IOP48	Test for eSBC loss of Ethernet link and reconnection	• Remove the Ethernet link between the eSBC and CE router. Leave in this condition for at least 3 minutes. • Reconnect the Ethernet link and ensure that after approximately 2 minutes inbound and outbound calls are successful.	Pass With Caveat	It takes five minutes before Edgmarc EM6000 accepts inbound calls when MS Teams or the SIP Trunk becomes unreachable,. Five consecutive Options (pings) are required from the EdgeMarc before it declares a trunk is available or clears the unreachable alarm.)
IOP49	Test for the Primary SBC loss	** Contact MSL engineer to carry out the following ** • On the Primary SBC, carry out the ALLSTOP command to disable the SBC. • Make a call from the IP-PBX line to a PSTN Line. • Make sure that the call tries to route to the Primary SBC. On a non-response to INVITE, the eSBC re-routes the call to the Secondary SBC. • Wait for call answer. • Either party terminates call. ** Contact MSL engineer to carry out the following ** • Restart the Primary SBC.	Pass	

IOP51	Test for Call forward Internal Busy	Additional test to cover when vendors are using Microsoft Skype for Business 2015: • PBX Subscriber 1 makes a call to PBX Subscriber 2, so that the PSTN to call the PBX subscriber 1 is Busy. • PSTN calls PBX user 1. The call should automatically go to voicemail after 10 seconds when call forwarding is off. • If VM is on another PBX Internal Line, the call should go to voicemail. • PSTN user listens to the voiceMail announcement, and leaves a clear message for PBX Subscriber 1 in VM. • If forwarded to voicemail, the PSTN terminates the call after hearing the VM announcement. • If forwarded to another user, either party terminates the call after checking that speech is clear in both directions.	Pass	
IOP52	Test for Call forward internal on No Answer	Additional test to cover when vendors are using Microsoft Skype for Business 2015: • PSTN calls PBX user 1. • The PBX User 1 should not to answer the call. • The call should automatically go to voicemail (VM), which is in another internal PBX line if call forwarding is turned off. • The call automatically goes to voicemail after 10 seconds. • The PSTN terminates the call after hearing the VM announcement. • If call forwarding is ON, the call is forwarded to another PBX user internal. • Check the speech quality, and terminate the call after checking that speech is clear in both directions.	Pass	
IOP53	Test for making a call from a PBX to a PSTN	• Configure the eSBC to offer the T.38 in addition to G711A-law and G711-U law. • Make a call from the PBX to a PSTN. • Ensure the call is connected and dialog takes place for 10 minutes. • Check the Wireshark output. Confirm that the T.38 is not reflected in the protocol column after the call is connected for 7 minutes. • If T.38 is reflected in the protocol column, note it down.	Not-executed	Since MS Teams does not support Fax, configuring T.38 on the Edgemarc platform when using MS Teams is never required.

Appendix A

- If you need to send as Caller Number "Anonymous", you need to configure the next parameters Anonymous Profile in MS Teams:

Figure 13: Anonymous

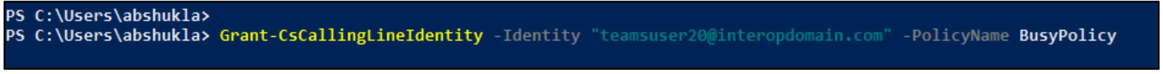


```
PS C:\Users\abshukla> New-CsCallingLineIdentity -Identity Anonymoustest -Descr
-EnableUserOverride $false_
```

```
PS C:\Users\abshukla>
PS C:\Users\abshukla> Grant-CsCallingLineIdentity -Identity "teamsuser20@inter
```

- Busy Profile is one of the default profile available on the MS Teams admin page. Admin can assign this profile to a particular user, using CLI or GUI. You need this configuration if you need to send a Busy Tone for busy calls:

Figure 14: Busy Tone



```
PS C:\Users\abshukla>
PS C:\Users\abshukla> Grant-CsCallingLineIdentity -Identity "teamsuser20@interopdomain.com" -PolicyName BusyPolicy
```