sansay™

# VSXi SBC & Microsoft Teams Direct Routing Configuration Guide

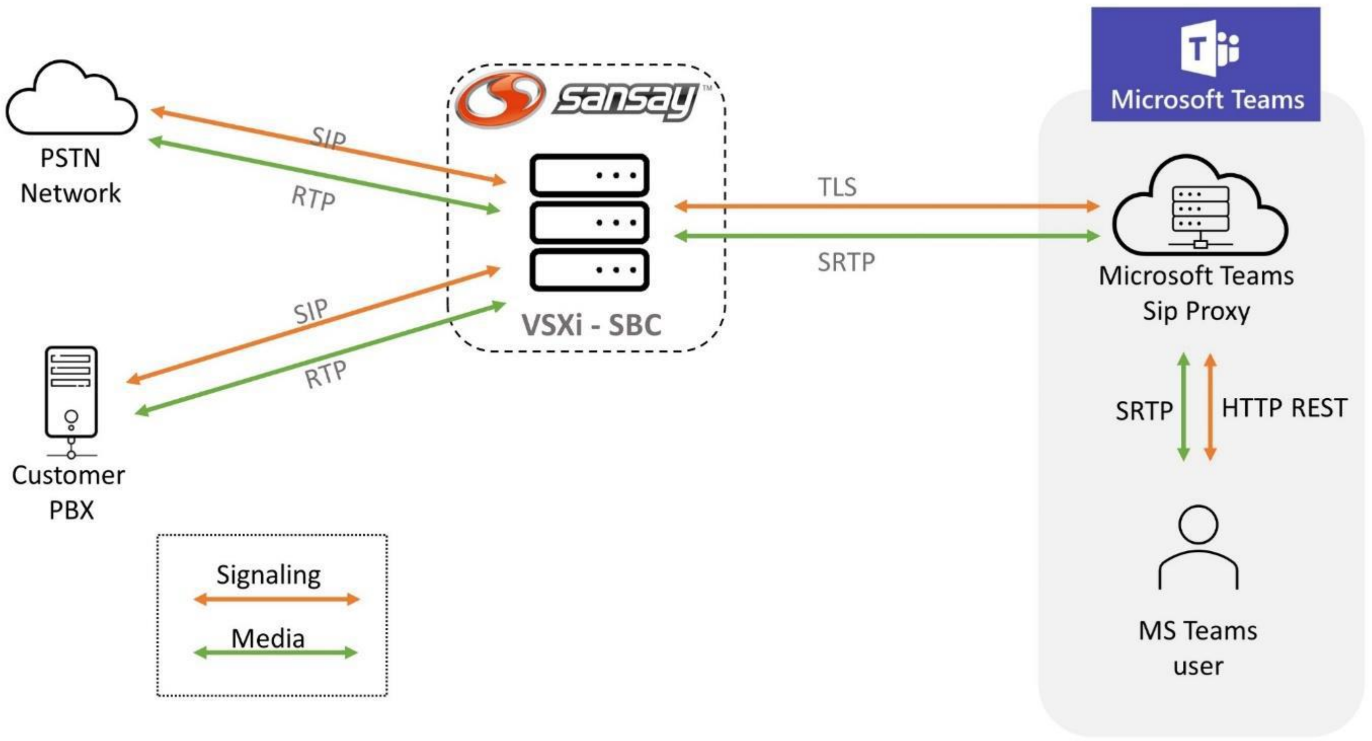
# OVERVIEW

Microsoft Teams Direct Routing allows you to connect your Session Border Controller (SBC) directly to Microsoft Phone System. With this capability, Microsoft Teams users will be able to make, receive, and transfer calls to and from landlines and mobile phones on the public switched telephone network (PSTN).

There are 2 way to interoperate MS Teams users with the PSTN:

- Using Microsoft Phone System and Calling Plans (Acquiring DID numbers directly with Microsoft)
- Using Microsoft Phone System and Direct Routing.

Sansay SBC and MS Teams Interconnection



This document is intended to guide you through the configuration process for setting Up Microsoft Teams Direct Routing to interconnect to Sansay VSXi SBC solution.

# REQUIREMENTS

## VSXi - SBC

- VSXi Code Version 10.5.1.354r27 or higher.
- SSL Certificate for SBC FQDN from Microsoft Authorized CA.
- External Media Server (for SRTP)

## Microsoft

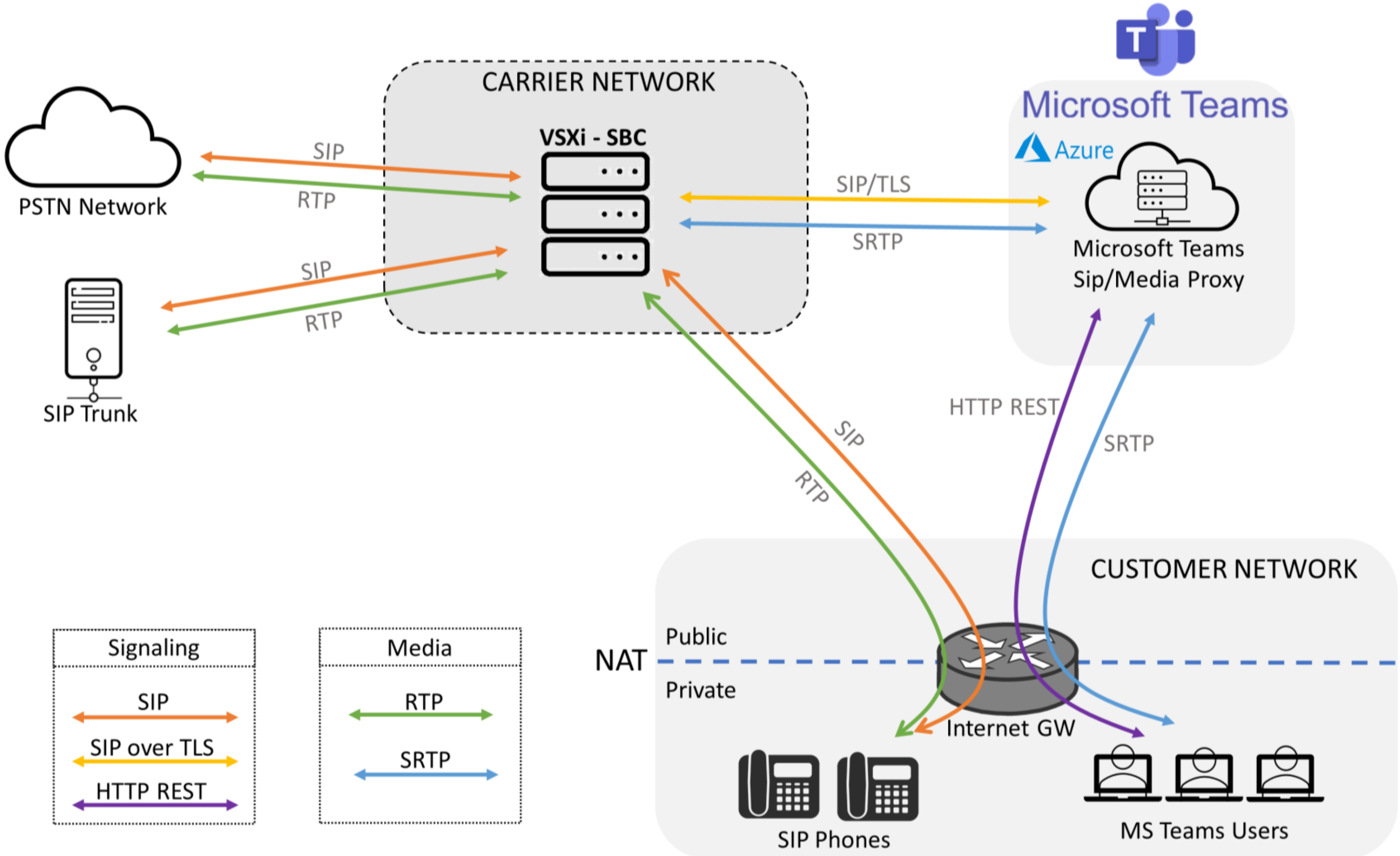
- Office 365 Organization Account
- Microsoft E5 or E3+Phone System license
- Microsoft Teams Users
- Fully Qualify Domain Name (FQDN) for SBC
- A DNS records for FQDN

# HIGH LEVEL CALL FLOW

## NON MEDIA BYPASS MODE

**Non-media bypass** is the default MS Teams Direct Routing operation mode. In this mode, both signaling and media flow between the SBC, the Microsoft Phone System, and the Teams client.

This approach does not affect call quality due to optimization of traffic flow within Microsoft networks in most geographies.



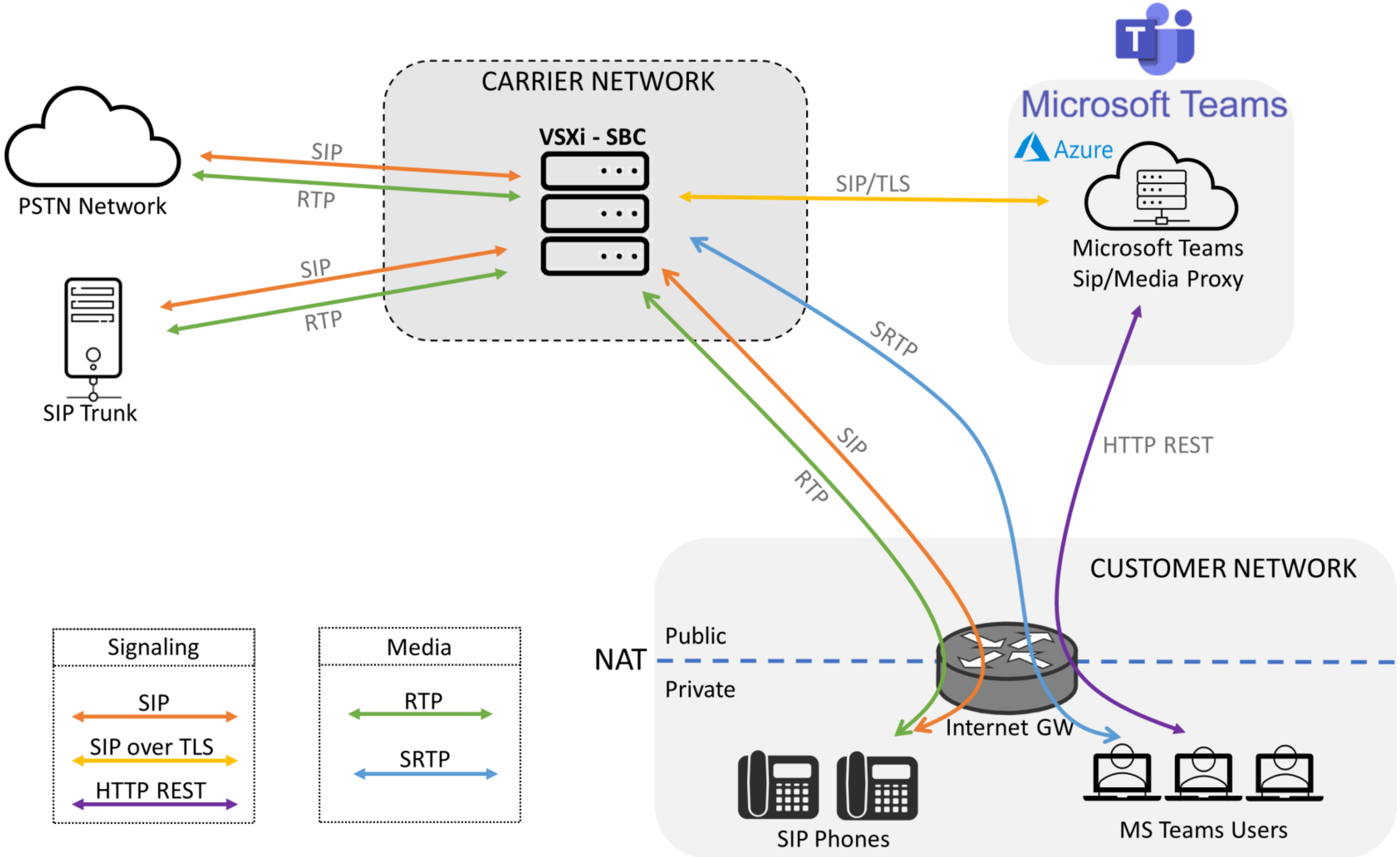
You can control media bypass for each SBC by using the **Set-CSOnlinePSTNGateway** command with the **-MediaBypass** parameter set to true or false

# HIGH LEVEL CALL FLOW

## MEDIA BYPASS MODE

**Media bypass** enables customer to shorten the path of media traffic and reduce the number of hops in transit for better performance. With media bypass, media is kept between the Session Border Controller (SBC) and the client instead of sending it via the Microsoft Phone System.

This mode is enabled at MS Teams Admin side.



You can control media bypass for each SBC by using the **Set-CSOnlinePSTNGateway** command with the **-MediaBypass** parameter set to true or false

# VSXi – MS TEAMS CONFIGURATION

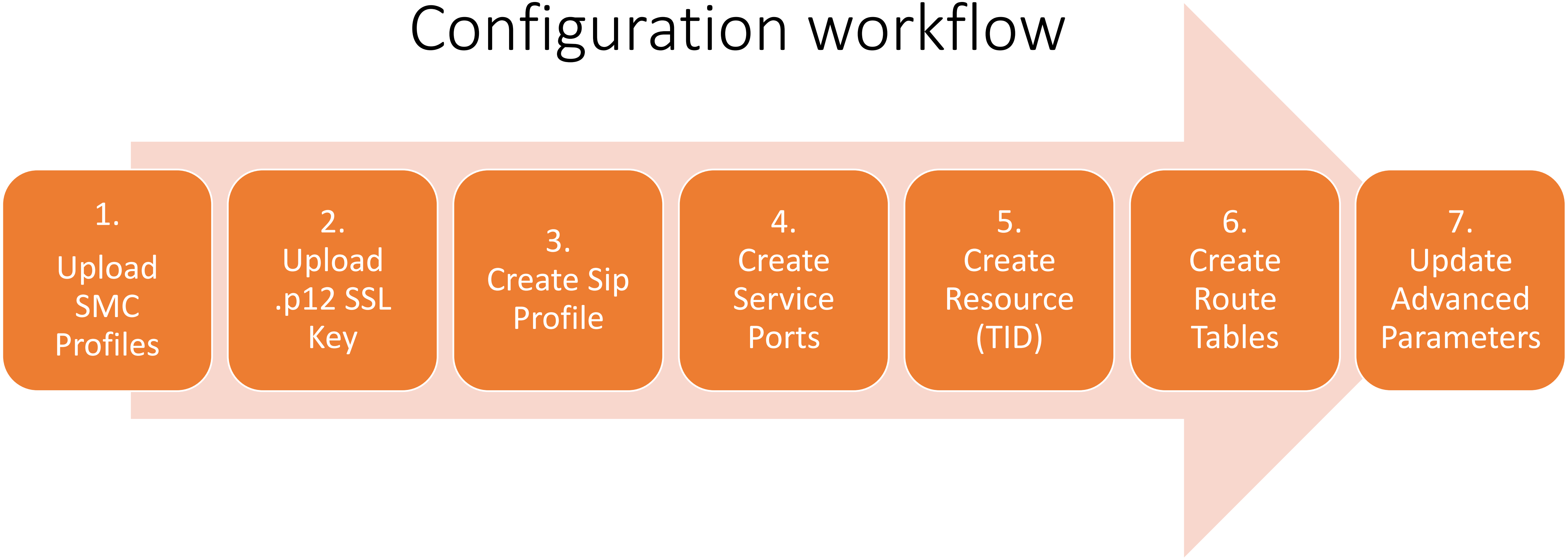
VSXi configuration for MS Teams Direct Routing relies on 7 elements:

- Service Ports (3 SP)
- Resources (2 TID for Microsoft Teams and N TID for each Microsoft Tenant)
- Routes (1 RT for MS Teams and 1 RT per Tenant)
- SMC Profiles (4 SMC)
- Sip Profile (1 SIP profile)
- Advanced Configuration Parameters
- VSXi Footprint for enabling ICE block (Sansay Support Team only).

We will cover each aspect and required config for each item.

# VSXi – MS TEAMS CONFIGURATION

## Configuration workflow



1. Upload SMC Profiles

2. Upload .p12 SSL Key

3. Create Sip Profile

4. Create Service Ports

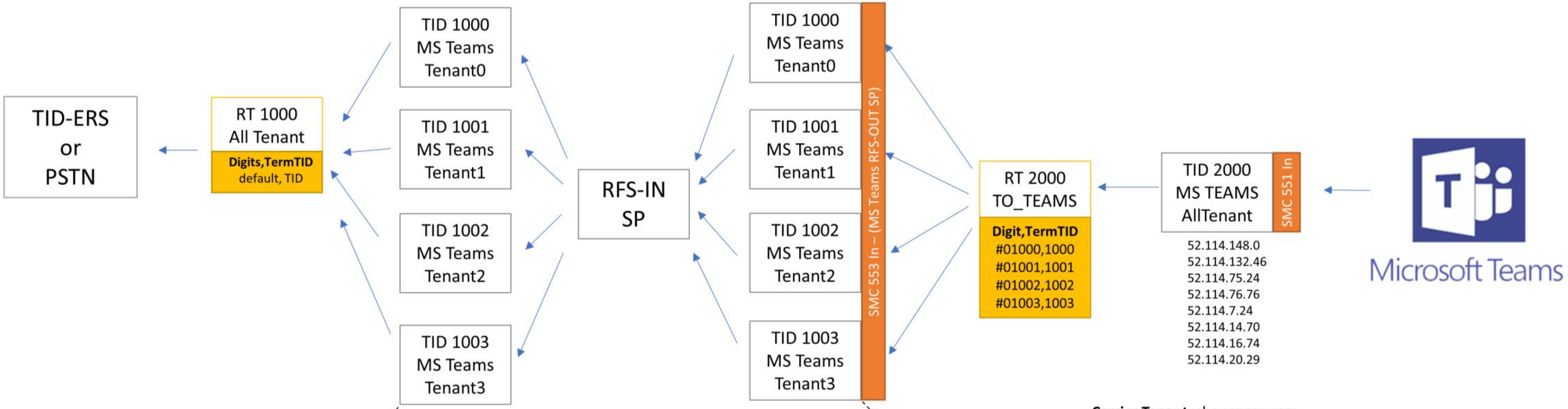
5. Create Resource (TID)

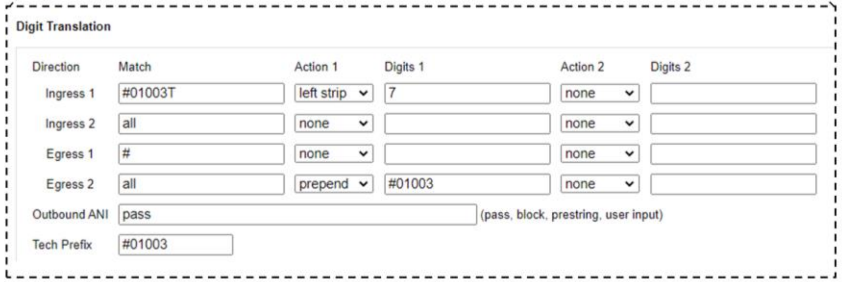
6. Create Route Tables

7. Update Advanced Parameters

# VSXI – MS TEAMS CONFIGURATION

Call Flow from MS Teams to PSTN (configuration example)





**Digit Translation**

| Direction | Match | Action 1 | Digits 1 | Action 2 | Digits 2 |
|---|---|---|---|---|---|
| Ingress 1 | #01003T | left strip | 7 | none | |
| Ingress 2 | all | none | | none | |
| Egress 1 | # | none | | none | |
| Egress 2 | all | prepend | #01003 | none | |

Outbound ANI: pass (pass, block, prestring, user input)

Tech Prefix: #01003

**Carrier Tenant:** sbc.sansay.com
**Customer Tenant:** tenantX.sbc.sansay.com

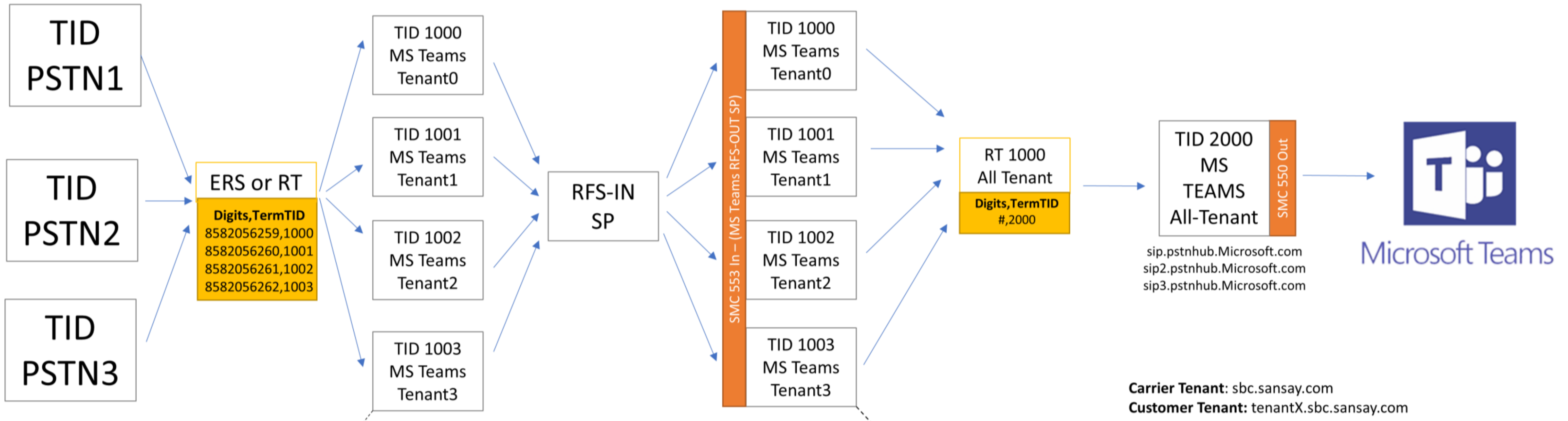
**Wildcard Certificate:**
CN=*.sbc.sansay.com, SAN:*.sbc.sansay.com, sbc.sansay.com

SMC Data File

```
#Tenant-fqdn,LocalIP,Tenant-Prefix
tenant0.sbc.sansay.com,54.193.191.186,#01000
tenant1.sbc.sansay.com,54.193.191.186,#01001
tenant2.sbc.sansay.com,54.193.191.186,#01002
tenant3.sbc.sansay.com,54.193.191.186,#01003
```

# VSXI – MS TEAMS CONFIGURATION

## Call Flow from PSTN to MS Teams (configuration example)



TID PSTN1

TID PSTN2

TID PSTN3

ERS or RT

**Digits,TermTID**
8582056259,1000
8582056260,1001
8582056261,1002
8582056262,1003

TID 1000 MS Teams Tenant0

TID 1001 MS Teams Tenant1

TID 1002 MS Teams Tenant2

TID 1003 MS Teams Tenant3

RFS-IN SP

SMC 553 In – (MS Teams RFS-OUT SP)

TID 1000 MS Teams Tenant0

TID 1001 MS Teams Tenant1

TID 1002 MS Teams Tenant2

TID 1003 MS Teams Tenant3

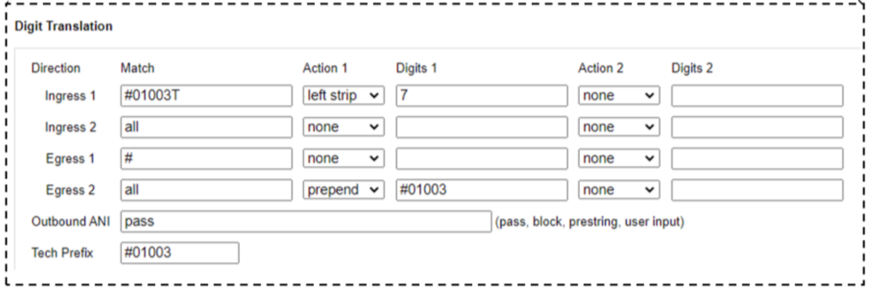
RT 1000 All Tenant

**Digits,TermTID**
#,2000

TID 2000 MS TEAMS All-Tenant

SMC 550 Out

sip.pstnhub.Microsoft.com
sip2.pstnhub.Microsoft.com
sip3.pstnhub.Microsoft.com



**Digit Translation**

| Direction | Match | Action 1 | Digits 1 | Action 2 | Digits 2 |
|---|---|---|---|---|---|
| Ingress 1 | #01003T | left strip | 7 | none | |
| Ingress 2 | all | none | | none | |
| Egress 1 | # | none | | none | |
| Egress 2 | all | prepend | #01003 | none | |

Outbound ANI: pass (pass, block, prestring, user input)

Tech Prefix: #01003

**Carrier Tenant**: sbc.sansay.com
**Customer Tenant:** tenantX.sbc.sansay.com

**Wildcard Certificate:**
CN=*.sbc.sansay.com, SAN:*.sbc.sansay.com, sbc.sansay.com

### SMC Data File

```
#Tenant-fqdn,LocalIP,Tenant-Prefix
tenant0.sbc.sansay.com,54.193.191.186,#01000
tenant1.sbc.sansay.com,54.193.191.186,#01001
tenant2.sbc.sansay.com,54.193.191.186,#01002
tenant3.sbc.sansay.com,54.193.191.186,#01003
```

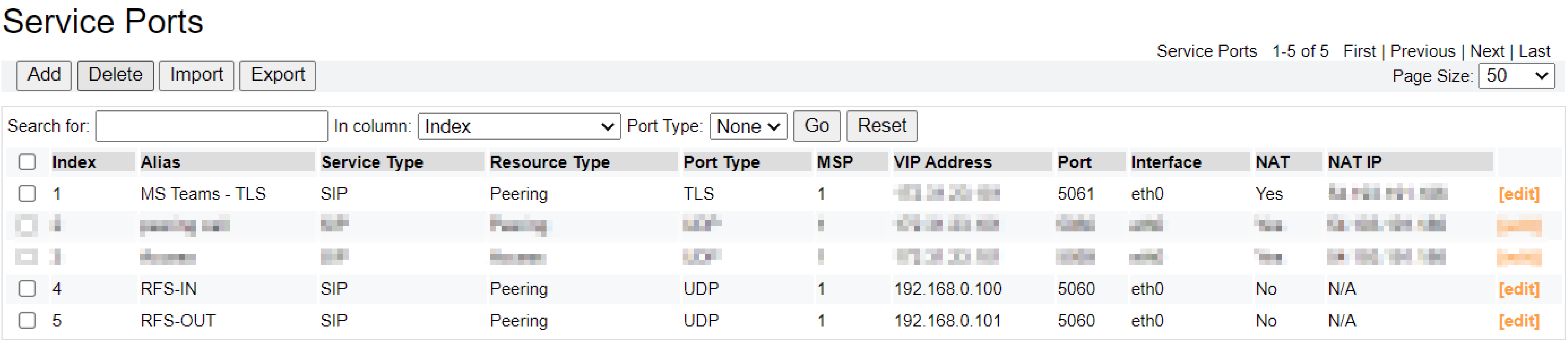
# VSXI CONFIGURATION – SERVICE PORT

Microsoft Teams Direct Routing configuration requires 3 Different Service Ports:

1- MS Teams – TLS

2- RFS-In Service Ports

3- RFS-Out MS Teams  (MS TeamsTenant )



## Service Ports

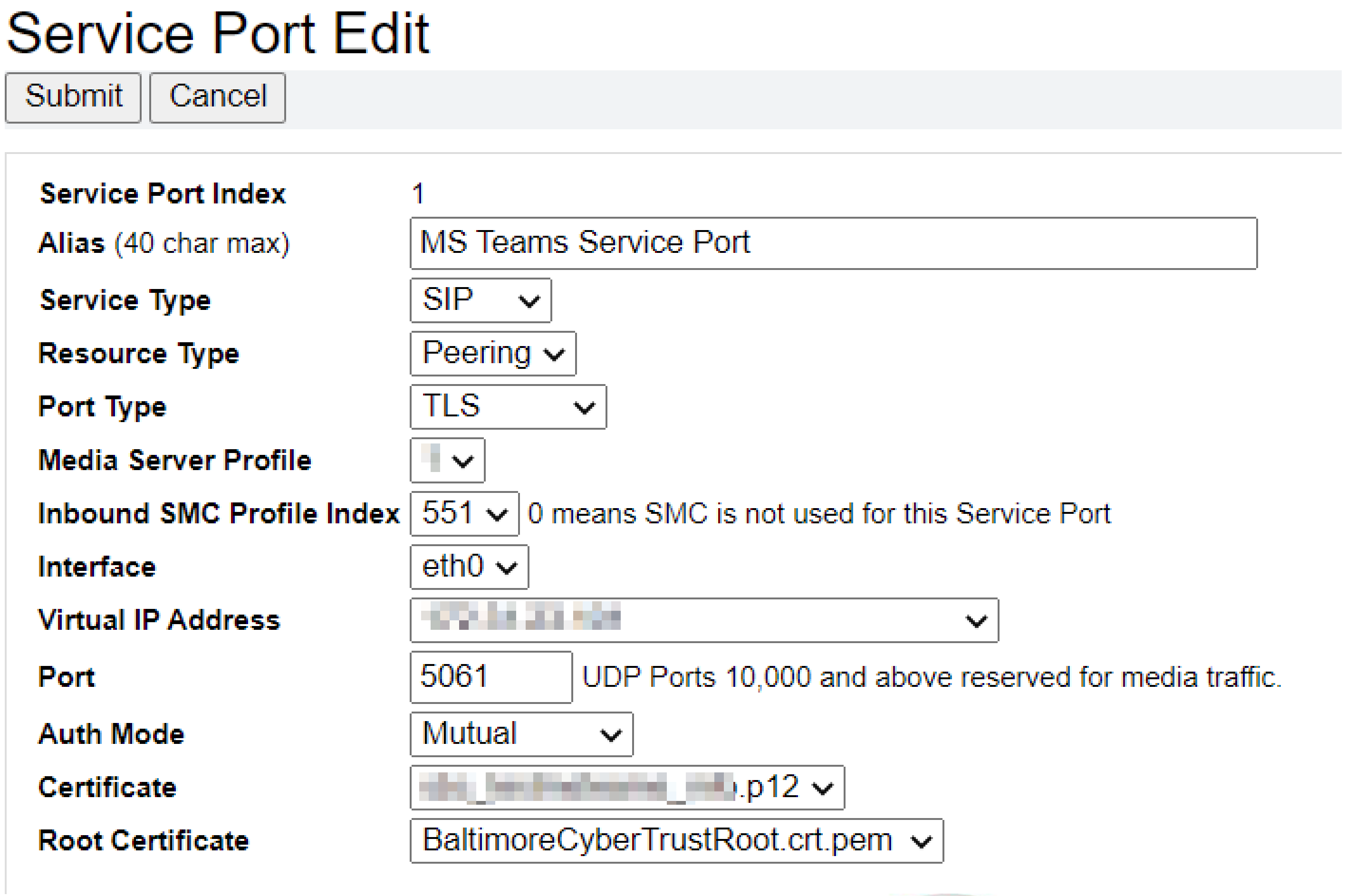
| □ | Index | Alias | Service Type | Resource Type | Port Type | MSP | VIP Address | Port | Interface | NAT | NAT IP | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | MS Teams - TLS | SIP | Peering | TLS | 1 | [redacted] | 5061 | eth0 | Yes | [redacted] | [edit] |
| □ | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| □ | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| □ | 4 | RFS-IN | SIP | Peering | UDP | 1 | 192.168.0.100 | 5060 | eth0 | No | N/A | [edit] |
| □ | 5 | RFS-OUT | SIP | Peering | UDP | 1 | 192.168.0.101 | 5060 | eth0 | No | N/A | [edit] |

# VSXI CONFIGURATION – SERVICE PORT

## Microsoft Teams Service Port

This is the Service Port facing Microsoft Phone System.

- Configured for TLS
- Auth Mode: Mutual
- SSL certificate for MS Teams FQDN (format .p12)
- BaltimoreCyberTrustRoot.cert as Root Cert
- Uses SMC profile 551.
- Media Server Profile with External Media Server.



### Service Port Edit

| | |
|---|---|
| **Service Port Index** | 1 |
| **Alias** (40 char max) | MS Teams Service Port |
| **Service Type** | SIP |
| **Resource Type** | Peering |
| **Port Type** | TLS |
| **Media Server Profile** | [redacted] |
| **Inbound SMC Profile Index** | 551 0 means SMC is not used for this Service Port |
| **Interface** | eth0 |
| **Virtual IP Address** | [redacted] |
| **Port** | 5061 UDP Ports 10,000 and above reserved for media traffic. |
| **Auth Mode** | Mutual |
| **Certificate** | [redacted].p12 |
| **Root Certificate** | BaltimoreCyberTrustRoot.crt.pem |

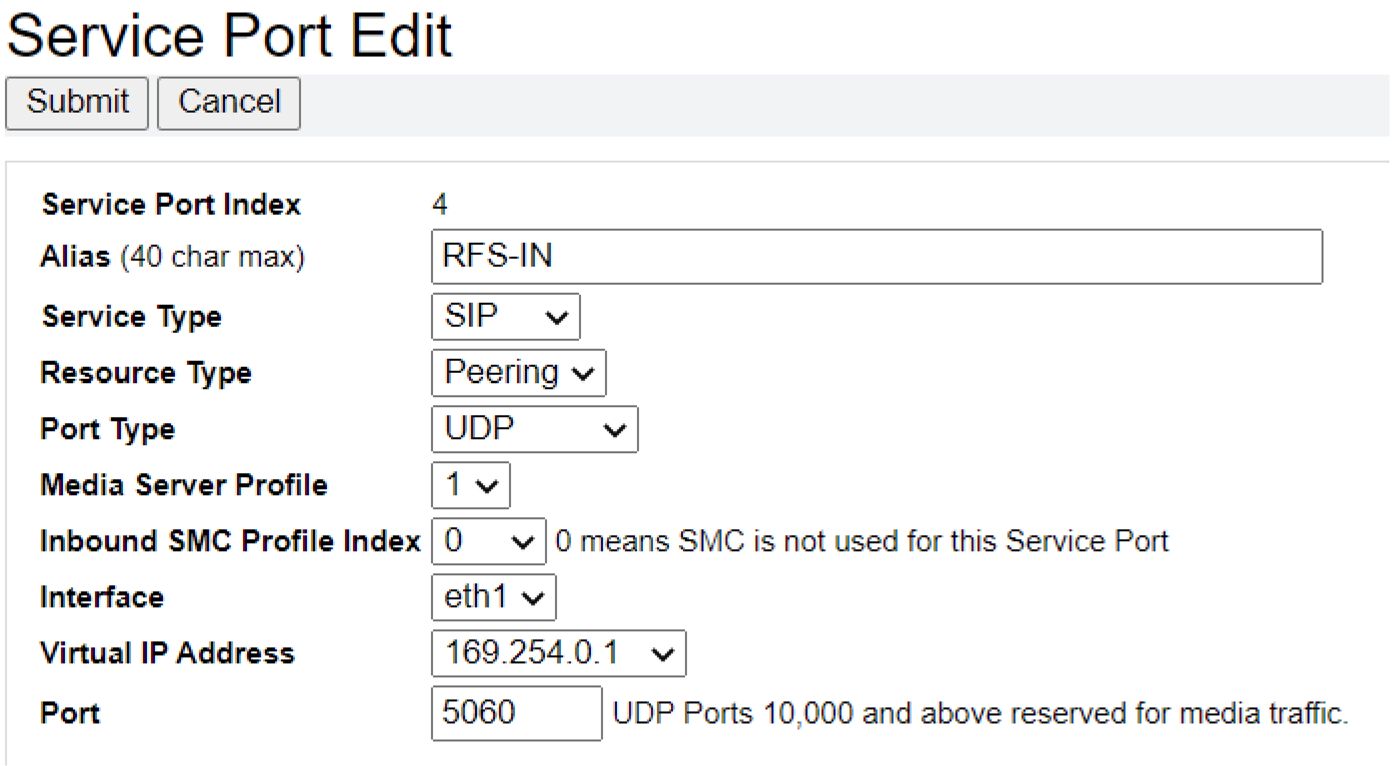
# VSXI CONFIGURATION – SERVICE PORT

## RFS-In Service Port

This Service Port is required to be able to process REFER method coming from MS Teams. This SIP method is called when HOLD or TRANSFER feature is used at MS Teams client.

This Service Port can use a fake VIP such as 169.254.0.1/30 as communication is only within Sansay VSXi domain. It can be attached to Private or Public Interface.

An advanced configuration setting will be required over this Service Port to enable RFS. (See advanced parameter section).



Service Port Edit

| | |
|---|---|
| Service Port Index | 4 |
| Alias (40 char max) | RFS-IN |
| Service Type | SIP |
| Resource Type | Peering |
| Port Type | UDP |
| Media Server Profile | 1 |
| Inbound SMC Profile Index | 0 — 0 means SMC is not used for this Service Port |
| Interface | eth1 |
| Virtual IP Address | 169.254.0.1 |
| Port | 5060 — UDP Ports 10,000 and above reserved for media traffic. |

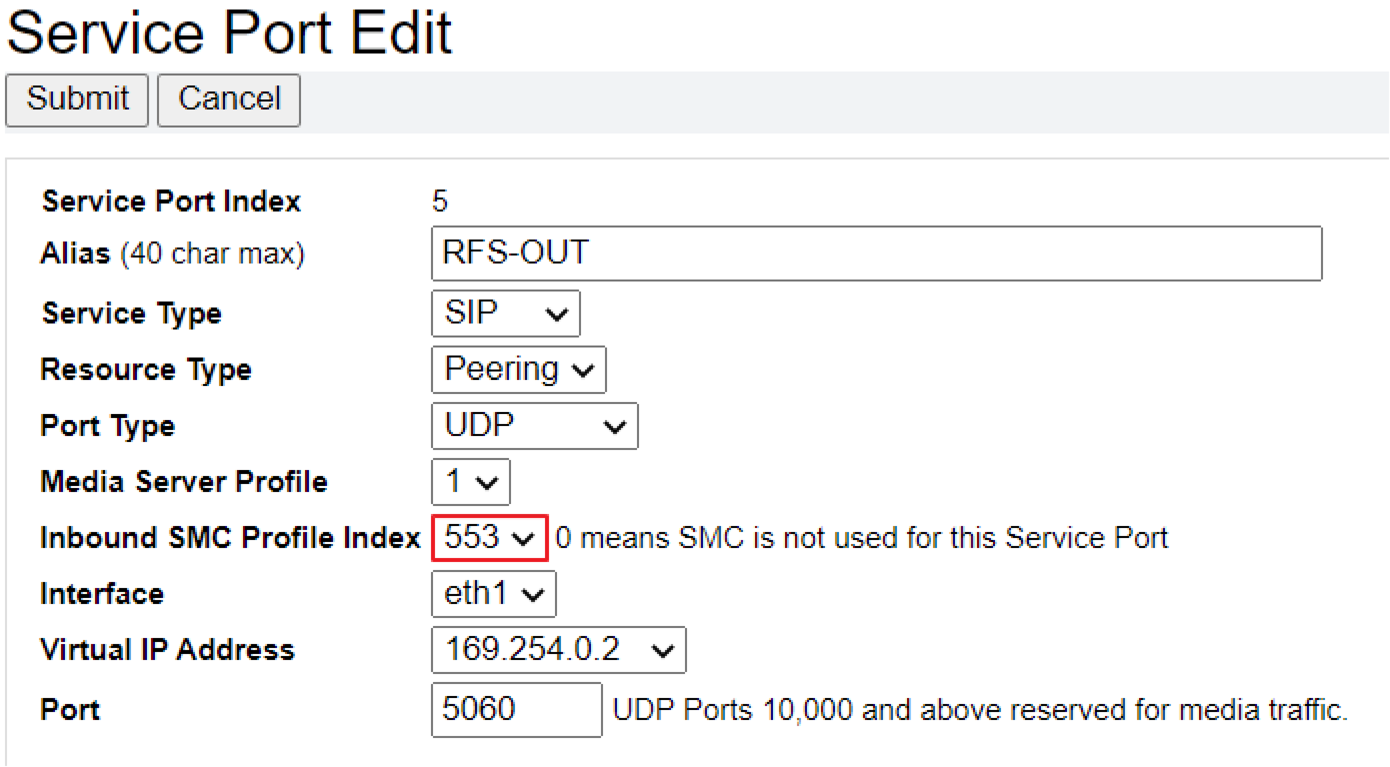
# VSXI CONFIGURATION – SERVICE PORT

## RFS-Out Service Port

RFS-Out Service Port also called MS Teams Tenant Service port will be used for your MS teams Tenant TID.  All of the MS Teams Tenant will be assigned to this same MS Teams Service Port.

This Service Port can use a fake VIP such as 169.254.0.2/30 as communication is only within Sansay VSXi domain. It can be attached to Private or Public Interface.

This Service Port uses SMC profile 553.
(check SMC profiles sections)



Service Port Edit

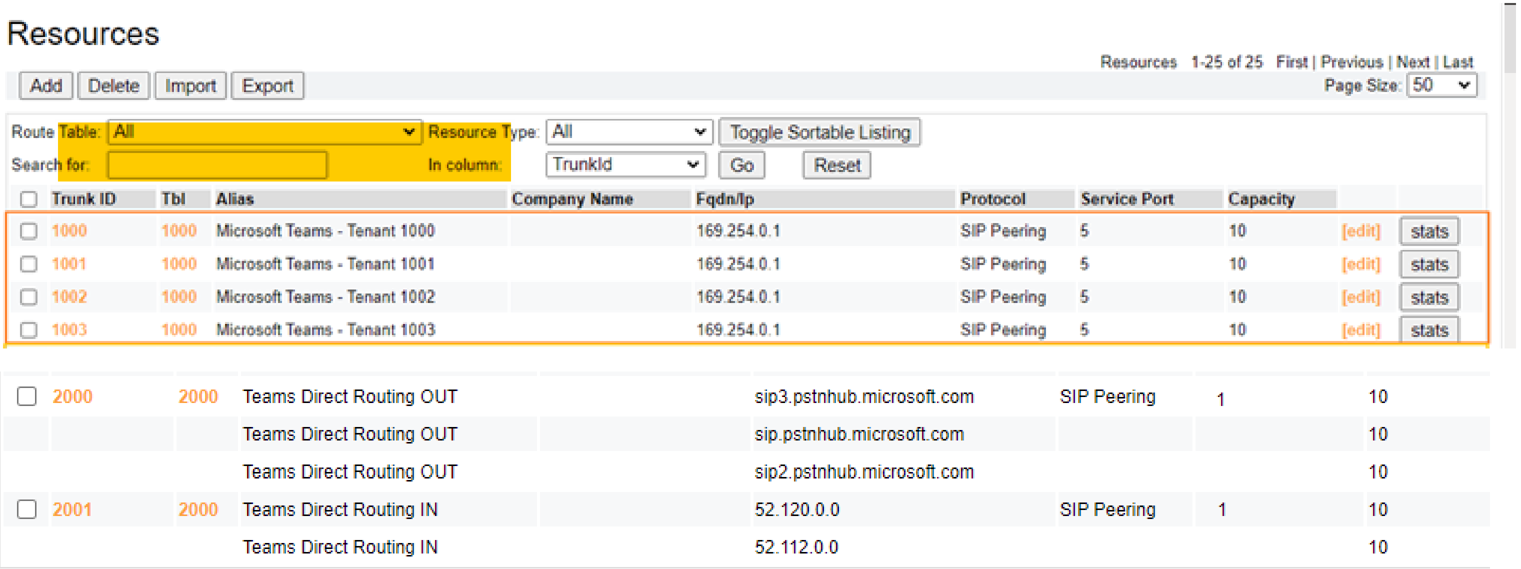
|  |  |
|---|---|
| **Service Port Index** | 5 |
| **Alias** (40 char max) | RFS-OUT |
| **Service Type** | SIP |
| **Resource Type** | Peering |
| **Port Type** | UDP |
| **Media Server Profile** | 1 |
| **Inbound SMC Profile Index** | 553 0 means SMC is not used for this Service Port |
| **Interface** | eth1 |
| **Virtual IP Address** | 169.254.0.2 |
| **Port** | 5060 UDP Ports 10,000 and above reserved for media traffic. |

# VSXI CONFIGURATION – RESOURCES

Resource section configuration requires at least 3 new Resources for MS Teams. The number of Resources will be proportional to the number of MS Teams Tenant to be configured.

The picture provides an example where there are 4 different tenant configured (1000 – 1003). Each MS Teams tenant will have its own domain but domain section is covered at SMC profiles config section.

You can have as many MS teams Tenant needed, but only 1 MS Teams OUT and 1 MS Teams IN shared by all MS Teams Tenant are needed.



Resources

Resources 1-25 of 25 First | Previous | Next | Last

Page Size: 50

Route Table: All Resource Type: All

Search for: In column: TrunkId

| □ | Trunk ID | Tbl | Alias | Company Name | Fqdn/Ip | Protocol | Service Port | Capacity | | |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | 1000 | 1000 | Microsoft Teams - Tenant 1000 | | 169.254.0.1 | SIP Peering | 5 | 10 | [edit] | stats |
| □ | 1001 | 1000 | Microsoft Teams - Tenant 1001 | | 169.254.0.1 | SIP Peering | 5 | 10 | [edit] | stats |
| □ | 1002 | 1000 | Microsoft Teams - Tenant 1002 | | 169.254.0.1 | SIP Peering | 5 | 10 | [edit] | stats |
| □ | 1003 | 1000 | Microsoft Teams - Tenant 1003 | | 169.254.0.1 | SIP Peering | 5 | 10 | [edit] | stats |
| □ | 2000 | 2000 | Teams Direct Routing OUT | | sip3.pstnhub.microsoft.com | SIP Peering | 1 | 10 | | |
| | | | Teams Direct Routing OUT | | sip.pstnhub.microsoft.com | | | 10 | | |
| | | | Teams Direct Routing OUT | | sip2.pstnhub.microsoft.com | | | 10 | | |
| □ | 2001 | 2000 | Teams Direct Routing IN | | 52.120.0.0 | SIP Peering | 1 | 10 | | |
| | | | Teams Direct Routing IN | | 52.112.0.0 | | | 10 | | |

In the next slides we will be covering specifics from this 2 type of Resources: MS Teams & MS Tenant

# VSXI CONFIGURATION – RESOURCES

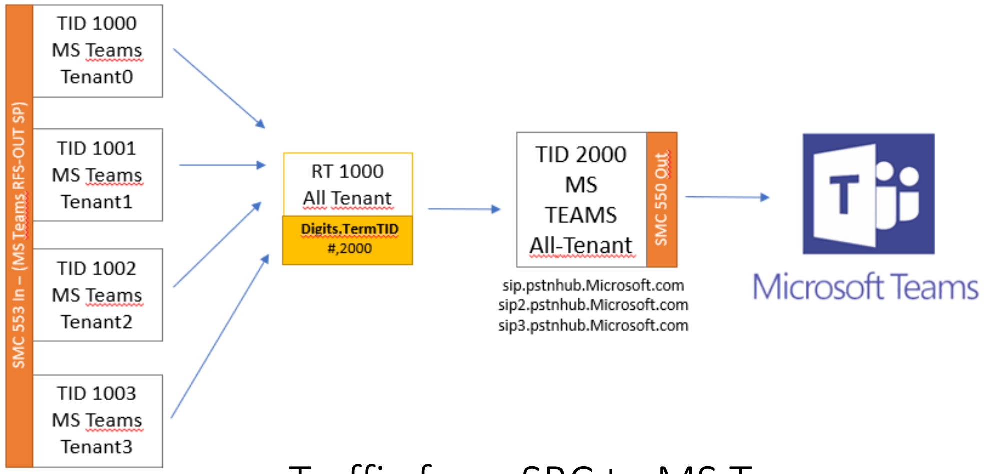
## MS Teams Resource

This is the TID configured to send/receive traffic from Microsoft SIP Proxy.

This resource uses the TLS Service Port with MS Teams certificate and it is also configured with SRTP enabled.

This resource is shared across multiple Microsoft Tenant as Microsoft Sip Proxy IPs are the same for any Microsoft Teams Tenant. Microsoft and VSXi will be able to distinguish each tenant traffic based on Contact domain information which must include the domain name for the MS Teams Tenant.

At VSXi MS Teams tenant fqdn is configured under SMC Data File which will be covered in a later section.



SMC 553 In – (MS Teams RFS-OUT SP)

TID 1000 MS Teams Tenant0

TID 1001 MS Teams Tenant1

TID 1002 MS Teams Tenant2

TID 1003 MS Teams Tenant3

RT 1000 All Tenant

Digits,TermTID #,2000

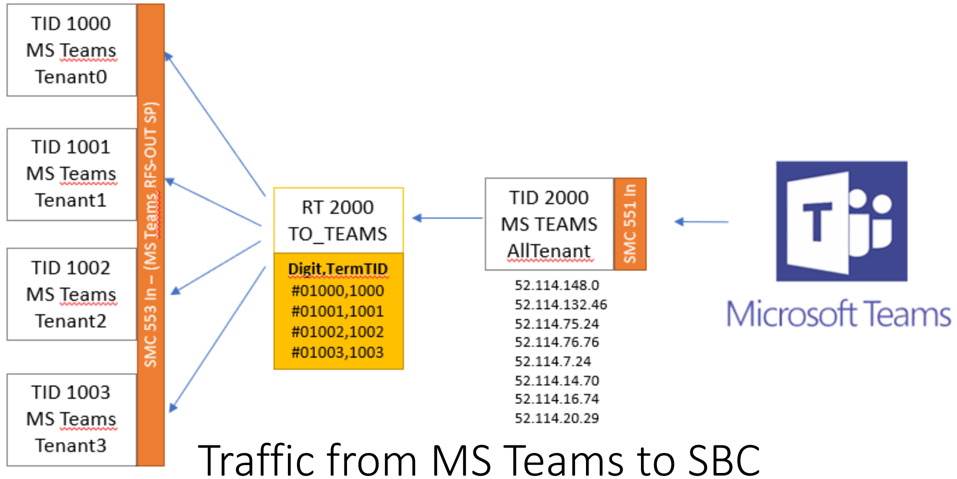
TID 2000 MS TEAMS All-Tenant

SMC 550 Out

sip.pstnhub.Microsoft.com
sip2.pstnhub.Microsoft.com
sip3.pstnhub.Microsoft.com

Microsoft Teams

Traffic from SBC to MS Teams



TID 1000 MS Teams Tenant0

TID 1001 MS Teams Tenant1

TID 1002 MS Teams Tenant2

TID 1003 MS Teams Tenant3

SMC 553 In – (MS Teams RFS-OUT SP)

RT 2000 TO_TEAMS

Digit,TermTID
#01000,1000
#01001,1001
#01002,1002
#01003,1003

TID 2000 MS TEAMS AllTenant

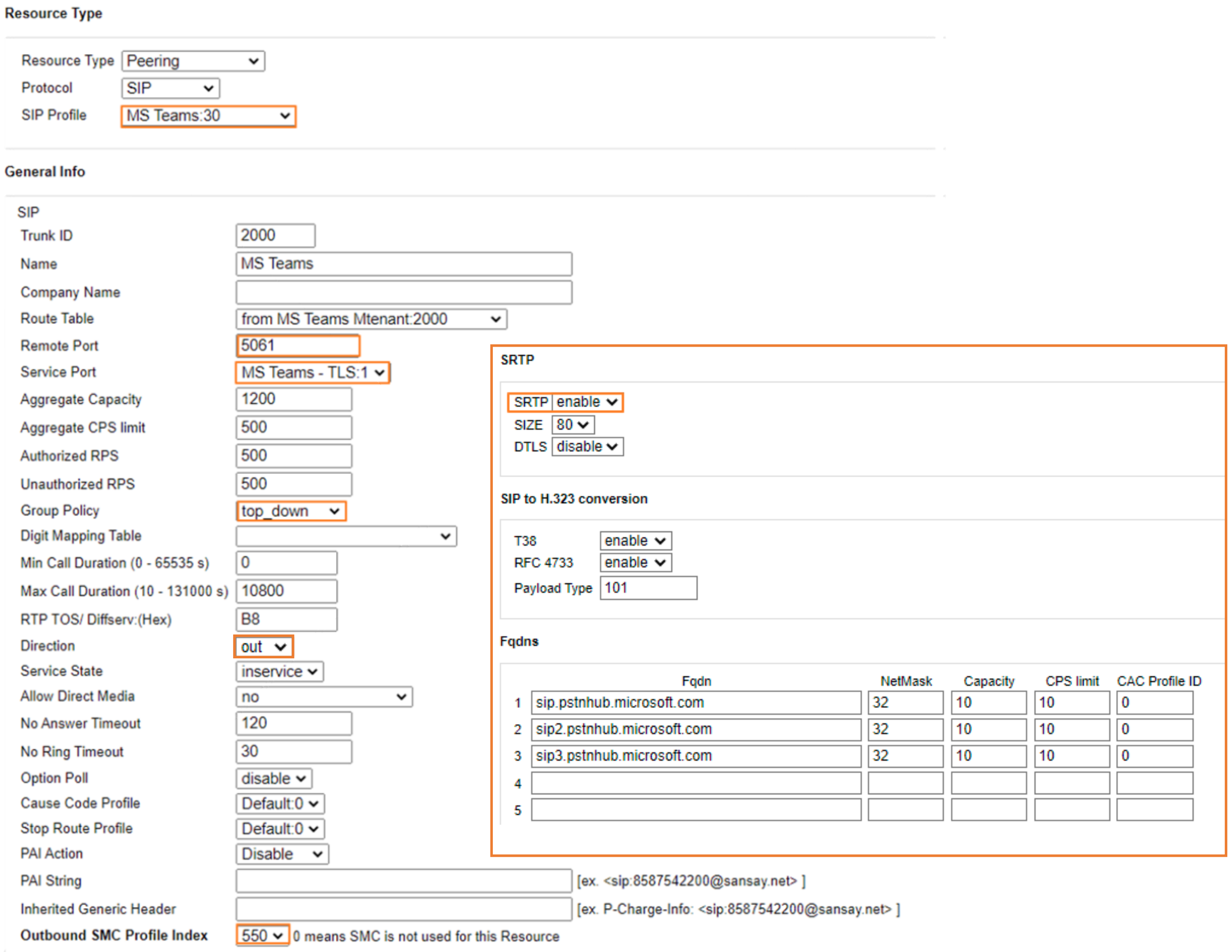
SMC 551 In

52.114.148.0
52.114.132.46
52.114.75.24
52.114.76.76
52.114.7.24
52.114.14.70
52.114.16.74
52.114.20.29

Microsoft Teams

Traffic from MS Teams to SBC

# VSXI CONFIGURATION – RESOURCES



**Resource Type**

| | |
|---|---|
| Resource Type | Peering |
| Protocol | SIP |
| SIP Profile | MS Teams:30 |

**General Info**

SIP

| | |
|---|---|
| Trunk ID | 2000 |
| Name | MS Teams |
| Company Name | |
| Route Table | from MS Teams Mtenant:2000 |
| Remote Port | 5061 |
| Service Port | MS Teams - TLS:1 |
| Aggregate Capacity | 1200 |
| Aggregate CPS limit | 500 |
| Authorized RPS | 500 |
| Unauthorized RPS | 500 |
| Group Policy | top_down |
| Digit Mapping Table | |
| Min Call Duration (0 - 65535 s) | 0 |
| Max Call Duration (10 - 131000 s) | 10800 |
| RTP TOS/ Diffserv:(Hex) | B8 |
| Direction | out |
| Service State | inservice |
| Allow Direct Media | no |
| No Answer Timeout | 120 |
| No Ring Timeout | 30 |
| Option Poll | disable |
| Cause Code Profile | Default:0 |
| Stop Route Profile | Default:0 |
| PAI Action | Disable |
| PAI String | [ex. <sip:8587542200@sansay.net> ] |
| Inherited Generic Header | [ex. P-Charge-Info: <sip:8587542200@sansay.net> ] |
| **Outbound SMC Profile Index** | 550 0 means SMC is not used for this Resource |

**SRTP**

| | |
|---|---|
| SRTP | enable |
| SIZE | 80 |
| DTLS | disable |

**SIP to H.323 conversion**

| | |
|---|---|
| T38 | enable |
| RFC 4733 | enable |
| Payload Type | 101 |

**Fqdns**

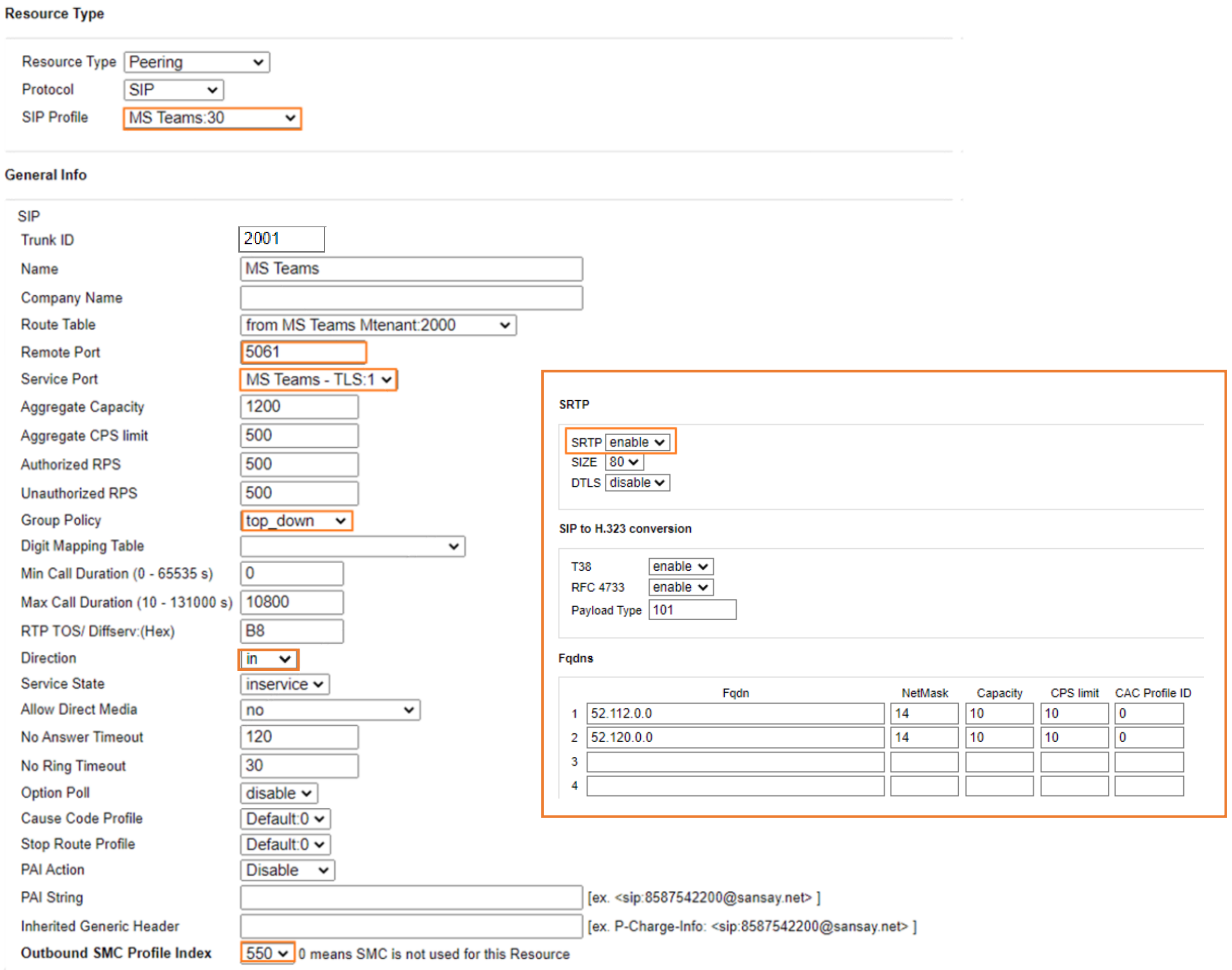
| | Fqdn | NetMask | Capacity | CPS limit | CAC Profile ID |
|---|---|---|---|---|---|
| 1 | sip.pstnhub.microsoft.com | 32 | 10 | 10 | 0 |
| 2 | sip2.pstnhub.microsoft.com | 32 | 10 | 10 | 0 |
| 3 | sip3.pstnhub.microsoft.com | 32 | 10 | 10 | 0 |
| 4 | | | | | |
| 5 | | | | | |

MS Teams **OUT** Resource Configuration

When creating the VSXi Resource for MS Teams Direct Routing please make sure to setup the MS Teams Resource parameters as follow:

- **Resource Type:** Peering
- **Protocol:** Sip
- **SIP Profile:** MS Teams SIP Profile
- **Remote Port:** 5061
- **Service Port:** MS Teams SP
- **Direction:** Out
- **Group Policy:** Top_down
- **Option Poll:** Disabled
- **Outbound SMC Profile Index:** 550
- **Codec Policy:** Transparent
- **SRTP:** Enabled

# VSXI CONFIGURATION – RESOURCES



**Resource Type**

| | |
|---|---|
| Resource Type | Peering |
| Protocol | SIP |
| SIP Profile | MS Teams:30 |

**General Info**

SIP

| | |
|---|---|
| Trunk ID | 2001 |
| Name | MS Teams |
| Company Name | |
| Route Table | from MS Teams Mtenant:2000 |
| Remote Port | 5061 |
| Service Port | MS Teams - TLS:1 |
| Aggregate Capacity | 1200 |
| Aggregate CPS limit | 500 |
| Authorized RPS | 500 |
| Unauthorized RPS | 500 |
| Group Policy | top_down |
| Digit Mapping Table | |
| Min Call Duration (0 - 65535 s) | 0 |
| Max Call Duration (10 - 131000 s) | 10800 |
| RTP TOS/ Diffserv:(Hex) | B8 |
| Direction | in |
| Service State | inservice |
| Allow Direct Media | no |
| No Answer Timeout | 120 |
| No Ring Timeout | 30 |
| Option Poll | disable |
| Cause Code Profile | Default:0 |
| Stop Route Profile | Default:0 |
| PAI Action | Disable |
| PAI String | [ex. <sip:8587542200@sansay.net> ] |
| Inherited Generic Header | [ex. P-Charge-Info: <sip:8587542200@sansay.net> ] |
| **Outbound SMC Profile Index** | 550 0 means SMC is not used for this Resource |

**SRTP**

| | |
|---|---|
| SRTP | enable |
| SIZE | 80 |
| DTLS | disable |

**SIP to H.323 conversion**

| | |
|---|---|
| T38 | enable |
| RFC 4733 | enable |
| Payload Type | 101 |

**Fqdns**

| | Fqdn | NetMask | Capacity | CPS limit | CAC Profile ID |
|---|---|---|---|---|---|
| 1 | 52.112.0.0 | 14 | 10 | 10 | 0 |
| 2 | 52.120.0.0 | 14 | 10 | 10 | 0 |
| 3 | | | | | |
| 4 | | | | | |

## MS Teams **IN** Resource Configuration

When creating the VSXi Resource for MS Teams Direct Routing please make sure to setup the MS Teams Resource parameters as follow:

- **Resource Type:** Peering
- **Protocol:** Sip
- **SIP Profile:** MS Teams SIP Profile
- **Remote Port:** 5061
- **Service Port:** MS Teams SP
- **Direction:** In
- **Group Policy:** Top_down
- **Option Poll:** Disabled
- **Outbound SMC Profile Index:** 550
- **Codec Policy:** Transparent
- **SRTP:** Enabled

# VSXI CONFIGURATION – RESOURCES

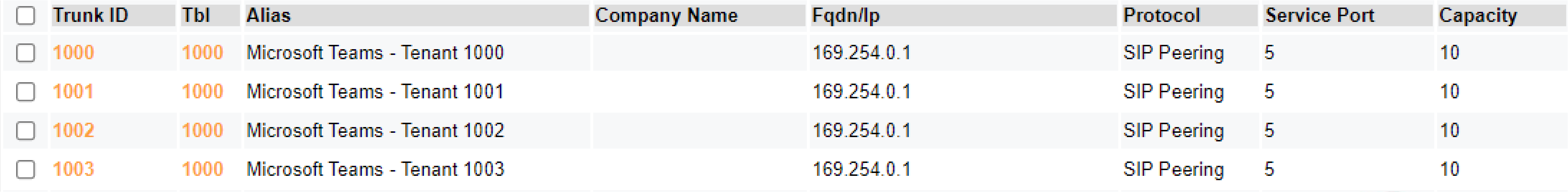
## MS Teams Tenant TID

This TIDs will serve as Microsoft Teams tenant TID. Multiple Tenant TID will be required when running multi-tenant approach.

Multitenant approach allows Carrier and Service Provider networks to have 1 wildcard ssl certificate and configure multiple customers with it.  There will be a carrier domain and multiple subdomain to call to/from each MS Teams Tenant. Additional information can be found here.

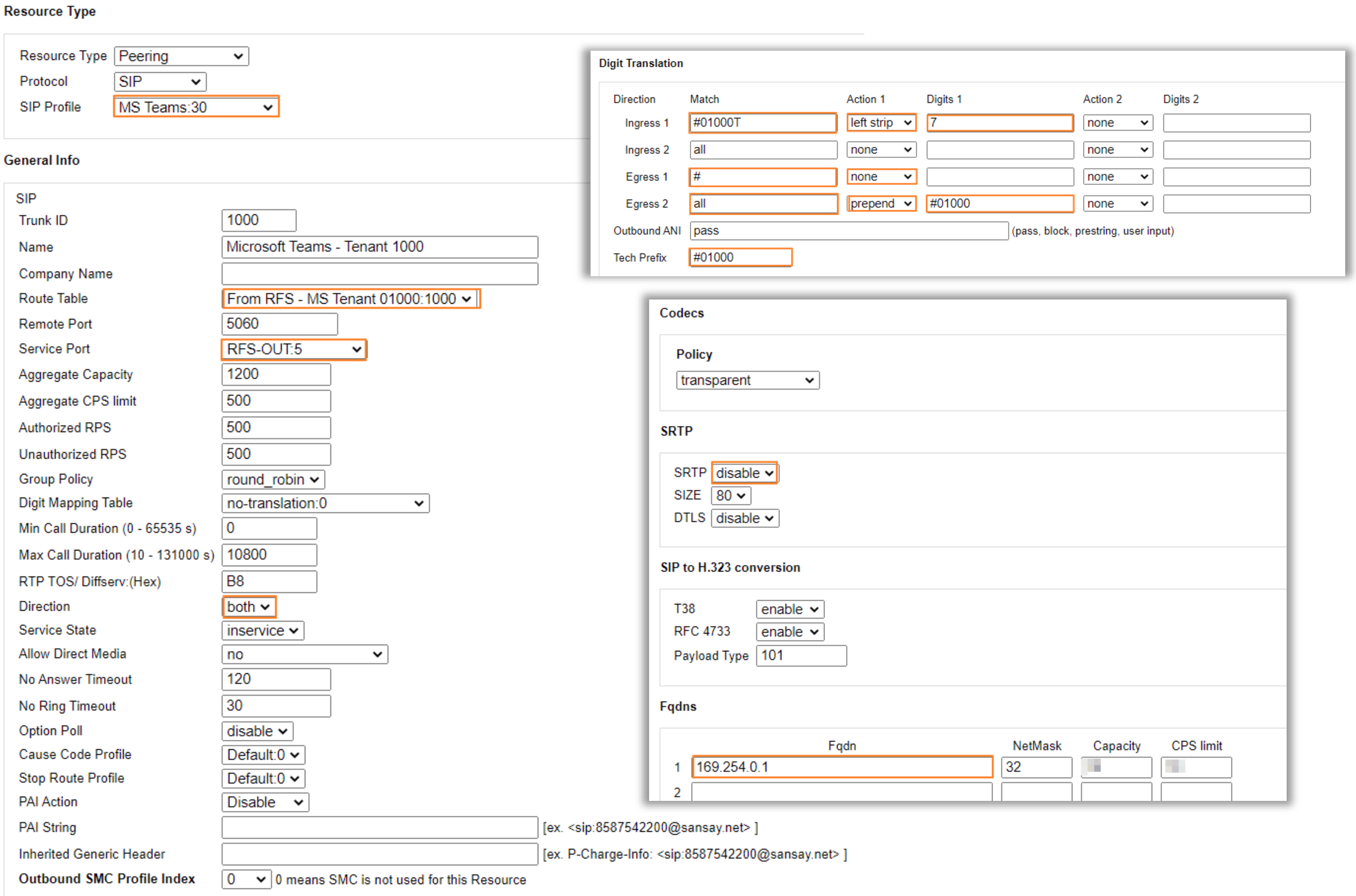
There should be a MS Teams Tenant TID per tenant. The MS Teams Tenant FQDN will be RFS-In Service Port IP.

All MS Teams tenant will be linked with the same Service Port (RFS-OUT).  A Tech-Prefix approach is needed to segment traffic.



| □ | Trunk ID | Tbl | Alias | Company Name | Fqdn/Ip | Protocol | Service Port | Capacity |
|---|---|---|---|---|---|---|---|---|
| □ | 1000 | 1000 | Microsoft Teams - Tenant 1000 |  | 169.254.0.1 | SIP Peering | 5 | 10 |
| □ | 1001 | 1000 | Microsoft Teams - Tenant 1001 |  | 169.254.0.1 | SIP Peering | 5 | 10 |
| □ | 1002 | 1000 | Microsoft Teams - Tenant 1002 |  | 169.254.0.1 | SIP Peering | 5 | 10 |
| □ | 1003 | 1000 | Microsoft Teams - Tenant 1003 |  | 169.254.0.1 | SIP Peering | 5 | 10 |

# VSXI CONFIGURATION – RESOURCES



**Resource Type**

| | |
|---|---|
| Resource Type | Peering |
| Protocol | SIP |
| SIP Profile | MS Teams:30 |

**General Info**

SIP

| | |
|---|---|
| Trunk ID | 1000 |
| Name | Microsoft Teams - Tenant 1000 |
| Company Name | |
| Route Table | From RFS - MS Tenant 01000:1000 |
| Remote Port | 5060 |
| Service Port | RFS-OUT:5 |
| Aggregate Capacity | 1200 |
| Aggregate CPS limit | 500 |
| Authorized RPS | 500 |
| Unauthorized RPS | 500 |
| Group Policy | round_robin |
| Digit Mapping Table | no-translation:0 |
| Min Call Duration (0 - 65535 s) | 0 |
| Max Call Duration (10 - 131000 s) | 10800 |
| RTP TOS/ Diffserv:(Hex) | B8 |
| Direction | both |
| Service State | inservice |
| Allow Direct Media | no |
| No Answer Timeout | 120 |
| No Ring Timeout | 30 |
| Option Poll | disable |
| Cause Code Profile | Default:0 |
| Stop Route Profile | Default:0 |
| PAI Action | Disable |
| PAI String | [ex. <sip:8587542200@sansay.net> ] |
| Inherited Generic Header | [ex. P-Charge-Info: <sip:8587542200@sansay.net> ] |
| **Outbound SMC Profile Index** | 0 0 means SMC is not used for this Resource |

**Digit Translation**

| Direction | Match | Action 1 | Digits 1 | Action 2 | Digits 2 |
|---|---|---|---|---|---|
| Ingress 1 | #01000T | left strip | 7 | none | |
| Ingress 2 | all | none | | none | |
| Egress 1 | # | none | | none | |
| Egress 2 | all | prepend | #01000 | none | |

| | |
|---|---|
| Outbound ANI | pass (pass, block, prestring, user input) |
| Tech Prefix | #01000 |

**Codecs**

**Policy**

transparent

**SRTP**

| | |
|---|---|
| SRTP | disable |
| SIZE | 80 |
| DTLS | disable |

**SIP to H.323 conversion**

| | |
|---|---|
| T38 | enable |
| RFC 4733 | enable |
| Payload Type | 101 |

**Fqdns**

| | Fqdn | NetMask | Capacity | CPS limit |
|---|---|---|---|---|
| 1 | 169.254.0.1 | 32 | | |
| 2 | | | | |

## MS Teams Tenant TID Configuration

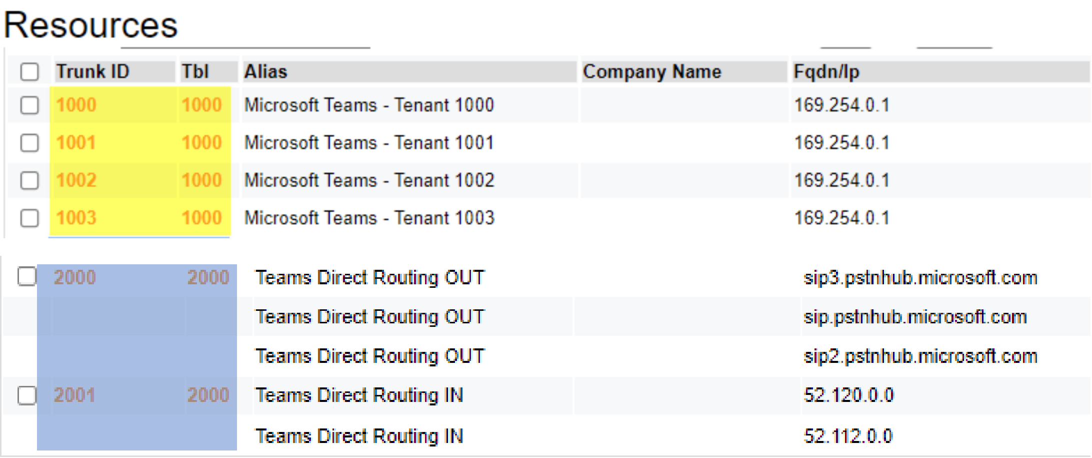
- Use RFS-OUT Service Port
- Use MS Teams Sip Profile
- Tech Prefix should match Prefix from SMC data File
- Fqdn will be RFS-IN Service Port IP (e.g. 169.254.0.1)
- Options Polls Disabled
- Digit Translation must be set as the example using tech id.

# VSXI CONFIGURATION – ROUTES

VSXi MS Teams configuration requires the following Route tables array:

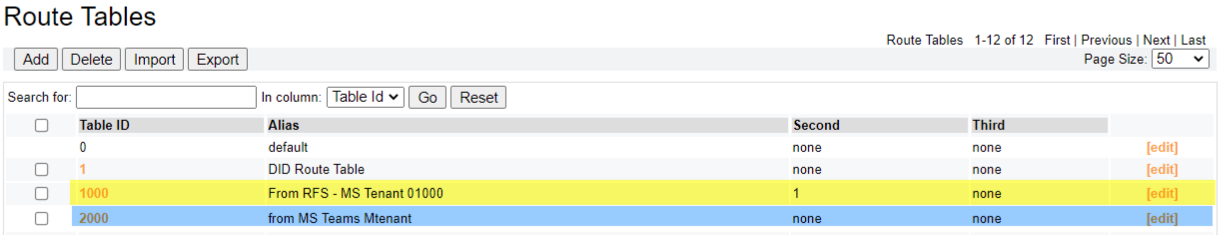
1- A route table (1) for MS Teams TID.
2- A Route table (1) for the MS Tenant TID.

Recommendation is to use same Trunk id reference for the route table. So if you MS teams TID is 2000, use RT 2000 for it.



Resources

| □ | Trunk ID | Tbl | Alias | Company Name | Fqdn/Ip |
|---|---|---|---|---|---|
| □ | 1000 | 1000 | Microsoft Teams - Tenant 1000 | | 169.254.0.1 |
| □ | 1001 | 1000 | Microsoft Teams - Tenant 1001 | | 169.254.0.1 |
| □ | 1002 | 1000 | Microsoft Teams - Tenant 1002 | | 169.254.0.1 |
| □ | 1003 | 1000 | Microsoft Teams - Tenant 1003 | | 169.254.0.1 |
| □ | 2000 | 2000 | Teams Direct Routing OUT | | sip3.pstnhub.microsoft.com |
| | | | Teams Direct Routing OUT | | sip.pstnhub.microsoft.com |
| | | | Teams Direct Routing OUT | | sip2.pstnhub.microsoft.com |
| □ | 2001 | 2000 | Teams Direct Routing IN | | 52.120.0.0 |
| | | | Teams Direct Routing IN | | 52.112.0.0 |



Route Tables

Route Tables 1-12 of 12 First | Previous | Next | Last

| □ | Table ID | Alias | Second | Third | |
|---|---|---|---|---|---|
| | 0 | default | none | none | [edit] |
| □ | 1 | DID Route Table | none | none | [edit] |
| □ | 1000 | From RFS - MS Tenant 01000 | 1 | none | [edit] |
| □ | 2000 | from MS Teams Mtenant | none | none | [edit] |

Notice MS Team Tenants Route table uses a secondary route where PSTN DID or default route should exist.

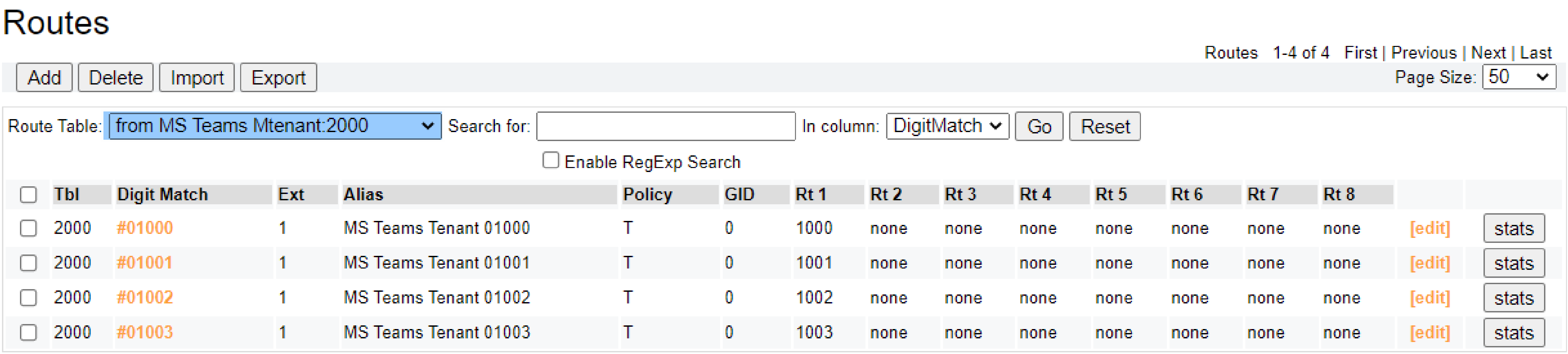
The next slides will describe what should be within MS Teams Route table and the MS Teams Tenant Route Table.

# VSXI CONFIGURATION – ROUTES

MS Teams resource is linked MS Teams Route table. This Route tabled should be provisioned with all Prefix defined in the SMC Data File as Customer Tenant Prefix ( See SMC data file section).

A digit route entry needs to be defined for each customer prefix pointing to the correspondent MS Teams Tenant TID (resource).

Here is an example of how this route table will look like:



Routes

Routes 1-4 of 4 First | Previous | Next | Last

Page Size: 50

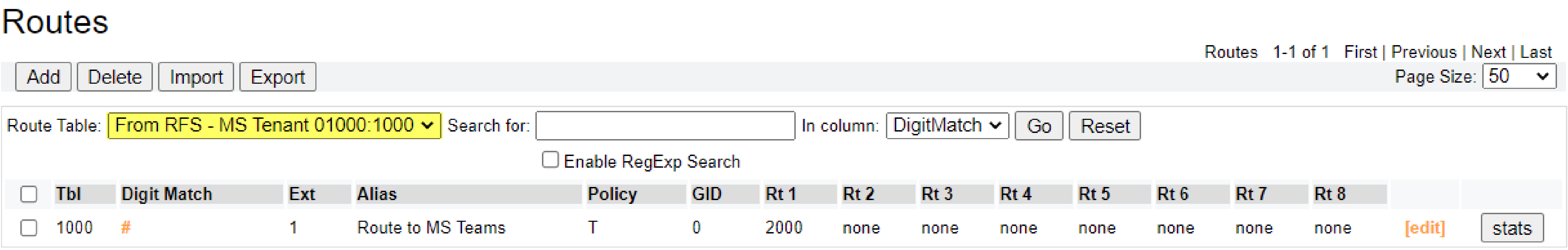
Route Table: from MS Teams Mtenant:2000 Search for: In column: DigitMatch

□ Enable RegExp Search

| □ | Tbl | Digit Match | Ext | Alias | Policy | GID | Rt 1 | Rt 2 | Rt 3 | Rt 4 | Rt 5 | Rt 6 | Rt 7 | Rt 8 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 2000 | #01000 | 1 | MS Teams Tenant 01000 | T | 0 | 1000 | none | none | none | none | none | none | none | [edit] | stats |
| □ | 2000 | #01001 | 1 | MS Teams Tenant 01001 | T | 0 | 1001 | none | none | none | none | none | none | none | [edit] | stats |
| □ | 2000 | #01002 | 1 | MS Teams Tenant 01002 | T | 0 | 1002 | none | none | none | none | none | none | none | [edit] | stats |
| □ | 2000 | #01003 | 1 | MS Teams Tenant 01003 | T | 0 | 1003 | none | none | none | none | none | none | none | [edit] | stats |

# VSXI CONFIGURATION – ROUTES

All MS Teams Tenant TIDs are linked with MS Tenant RT.
This route table has only one entry, it's a digit match entry with #.
Any call that comes with # should be sent to MS Teams TID (e.g. 2000).



## Routes

Routes 1-1 of 1 First | Previous | Next | Last

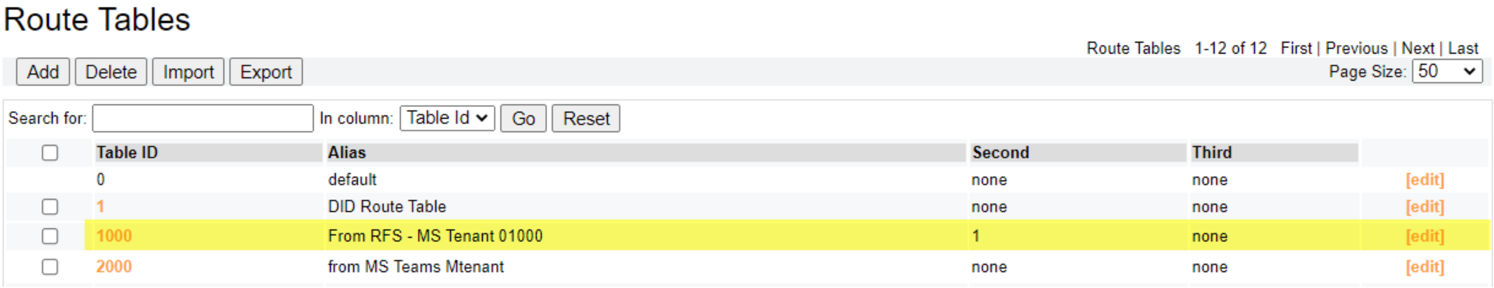
Page Size: 50

Route Table: From RFS - MS Tenant 01000:1000 Search for: In column: DigitMatch

□ Enable RegExp Search

| □ | Tbl | Digit Match | Ext | Alias | Policy | GID | Rt 1 | Rt 2 | Rt 3 | Rt 4 | Rt 5 | Rt 6 | Rt 7 | Rt 8 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 1000 | # | 1 | Route to MS Teams | T | 0 | 2000 | none | none | none | none | none | none | none | [edit] | stats |

MS Teams Tenant route table uses a secondary route table. The secondary route should have routes entry for Terminating call coming from Teams to PSTN. I could be default route towards Carrier TID.



## Route Tables

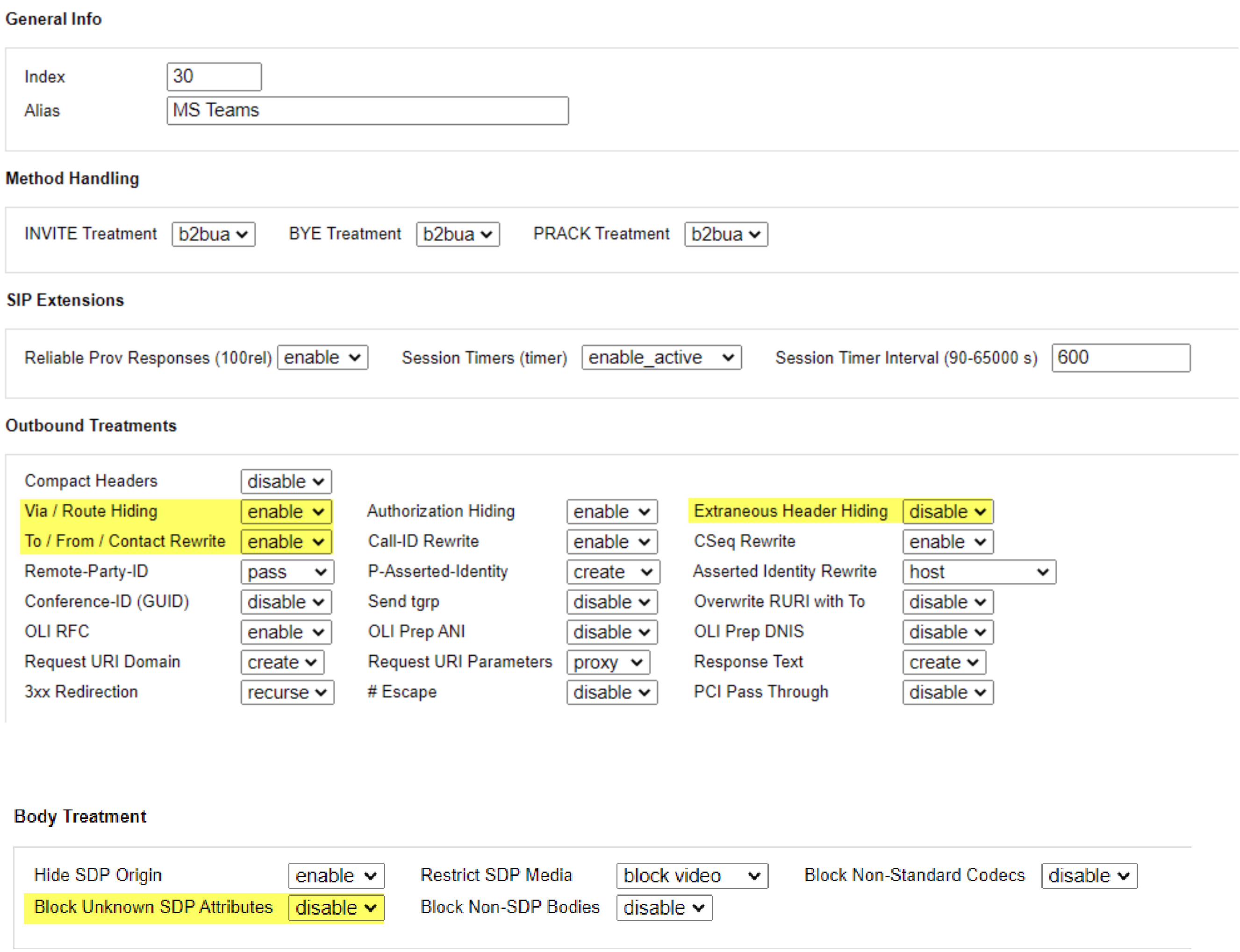
Route Tables 1-12 of 12 First | Previous | Next | Last

Page Size: 50

Search for: In column: Table Id

| □ | Table ID | Alias | Second | Third | |
|---|---|---|---|---|---|
| | 0 | default | none | none | [edit] |
| □ | 1 | DID Route Table | none | none | [edit] |
| □ | 1000 | From RFS - MS Tenant 01000 | 1 | none | [edit] |
| □ | 2000 | from MS Teams Mtenant | none | none | [edit] |

# VSXI CONFIGURATION – SIP PROFILE



### General Info

| | |
|---|---|
| Index | 30 |
| Alias | MS Teams |

### Method Handling

| | | | | | |
|---|---|---|---|---|---|
| INVITE Treatment | b2bua | BYE Treatment | b2bua | PRACK Treatment | b2bua |

### SIP Extensions

| | | | | | |
|---|---|---|---|---|---|
| Reliable Prov Responses (100rel) | enable | Session Timers (timer) | enable_active | Session Timer Interval (90-65000 s) | 600 |

### Outbound Treatments

| | | | | | |
|---|---|---|---|---|---|
| Compact Headers | disable | | | | |
| Via / Route Hiding | enable | Authorization Hiding | enable | Extraneous Header Hiding | disable |
| To / From / Contact Rewrite | enable | Call-ID Rewrite | enable | CSeq Rewrite | enable |
| Remote-Party-ID | pass | P-Asserted-Identity | create | Asserted Identity Rewrite | host |
| Conference-ID (GUID) | disable | Send tgrp | disable | Overwrite RURI with To | disable |
| OLI RFC | enable | OLI Prep ANI | disable | OLI Prep DNIS | disable |
| Request URI Domain | create | Request URI Parameters | proxy | Response Text | create |
| 3xx Redirection | recurse | # Escape | disable | PCI Pass Through | disable |

### Body Treatment

| | | | | | |
|---|---|---|---|---|---|
| Hide SDP Origin | enable | Restrict SDP Media | block video | Block Non-Standard Codecs | disable |
| Block Unknown SDP Attributes | disable | Block Non-SDP Bodies | disable | | |

## MS Teams Sip Profile configuration

Both type of TID (MS Teams & MS Tenant TID) should be configured with a new MS Teams SIP Profile.

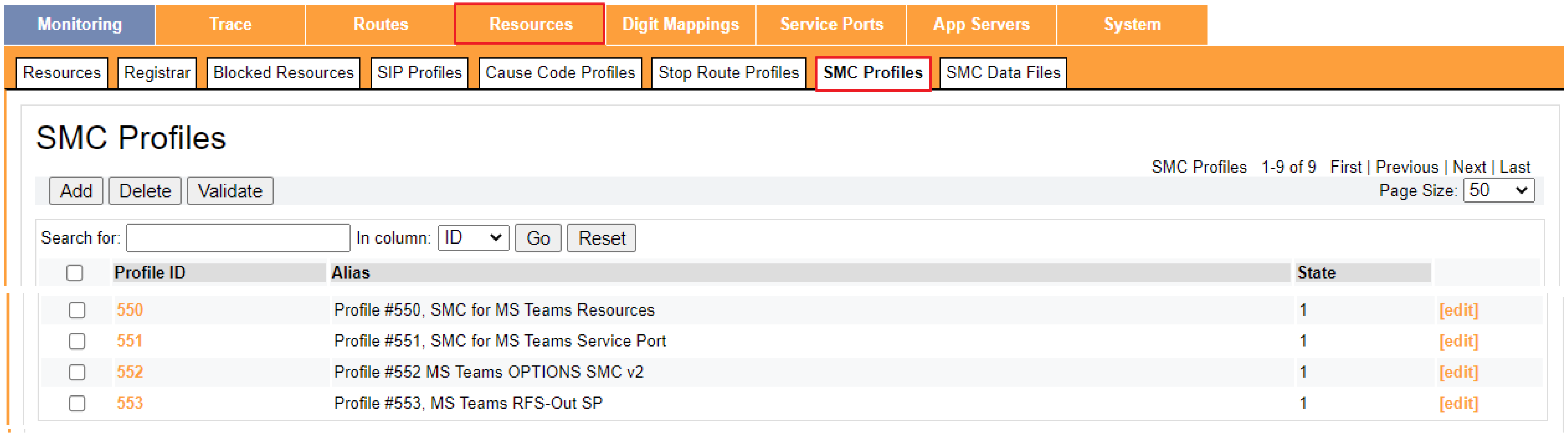
This SIP profile must be configured as example provided in the picture, specially for the fields highlighted in yellow. Not having them correctly set may result in break functionalities from MS teams or bad outcomes.

# VSXI CONFIGURATION – SMC Profiles

Microsoft Teams configuration requires the presence of 4 different SMC Profile + 1 SMC Data File:

SMC 550 – SMC configured under MS Teams Resource (Not MS Teams Tenant)
SMC 551 – SMC configured under MS Teams Service Port.
SMC 552 – SMC used for MS Teams Options Polls (its applied under /sg/sip.cfg  - adv. Parameteter)
SMC 553 – SMC configured under RFS-OUT Service Port.

Download SMC profiles from here.



## SMC Profiles

SMC Profiles 1-9 of 9 First | Previous | Next | Last

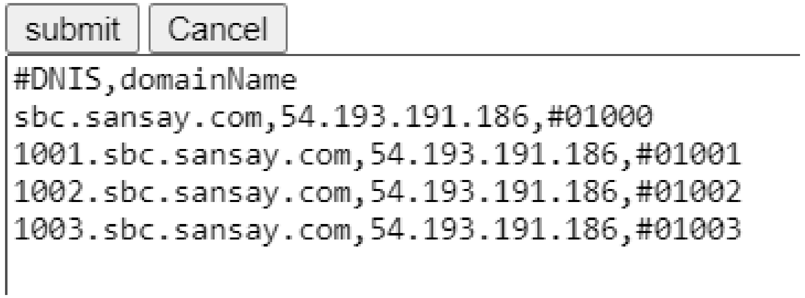
| □ | Profile ID | Alias | State | |
|---|---|---|---|---|
| □ | 550 | Profile #550, SMC for MS Teams Resources | 1 | [edit] |
| □ | 551 | Profile #551, SMC for MS Teams Service Port | 1 | [edit] |
| □ | 552 | Profile #552 MS Teams OPTIONS SMC v2 | 1 | [edit] |
| □ | 553 | Profile #553, MS Teams RFS-Out SP | 1 | [edit] |

# VSXI CONFIGURATION – SMC Data File

In addition to the SMC profile, MS Teams implementation requires an SMC Data file where the MS teams fqdns information is placed.

SMC Data file is compound of 3 different fields:

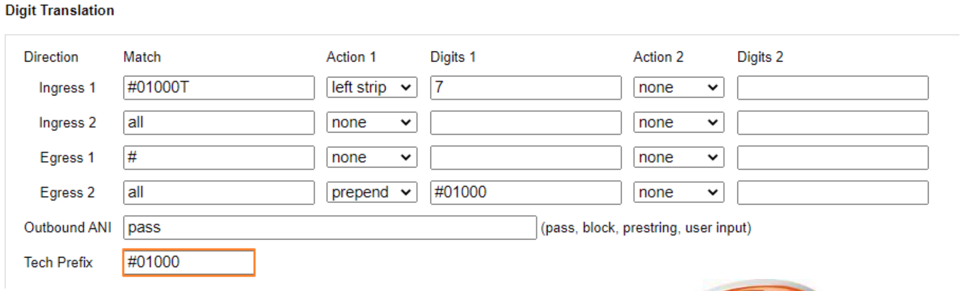
1- MS Teams Fqdn
2- Local TLS Service Port IP address
3- Prefix to identy the MS Teams Tenant



```
#DNIS,domainName
sbc.sansay.com,54.193.191.186,#01000
1001.sbc.sansay.com,54.193.191.186,#01001
1002.sbc.sansay.com,54.193.191.186,#01002
1003.sbc.sansay.com,54.193.191.186,#01003
```

Inside the SMC Data file we need to set the relation between each of MS teams fqdn (carrier and Tenant) and tech-Prefix specified for each MS Teams Tenant TID.

The prefix must always start with # followed by 5 digit. This prefix should match the the same tech-prefix that is configured under each MS teams tenant TID.



Digit Translation

| Direction | Match | Action 1 | Digits 1 | Action 2 | Digits 2 |
|---|---|---|---|---|---|
| Ingress 1 | #01000T | left strip | 7 | none | |
| Ingress 2 | all | none | | none | |
| Egress 1 | # | none | | none | |
| Egress 2 | all | prepend | #01000 | none | |

Outbound ANI: pass (pass, block, prestring, user input)

Tech Prefix: #01000

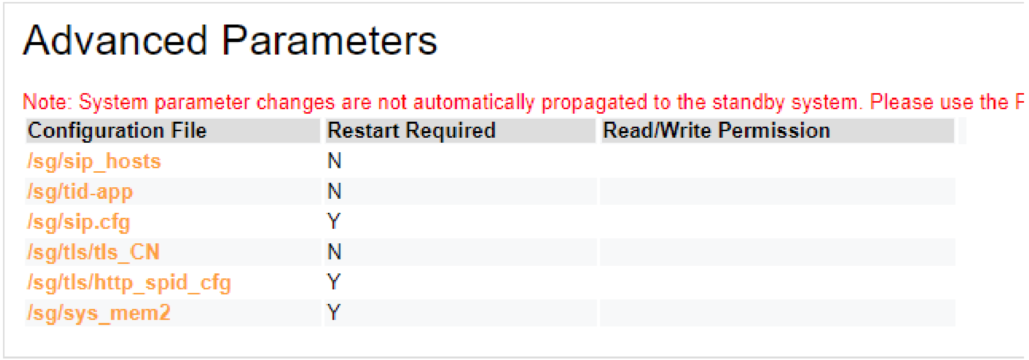
# VSXI CONFIGURATION – ADV PARAMETERS

The Advanced Parameters configurations allows VSXi end users to modify certain configuration elements that are not part of standard provisioning elements on the GUI.

Microsoft Teams configuration on the VSXI requires the presence of some Advanced Parameters for its proper working. Some of these Advanced Parameter's setting are reserved for Sansay Support only modification.

The List of the Advanced Parameter files that needs to be modified is the following:

- /sg/tid-app
- /sg/sip.cfg
- /sg/tls/tls_CN
- /sg/tls/http_spid_cfg
- /sg/sys_mem2



Advanced Parameters

Note: System parameter changes are not automatically propagated to the standby system. Please use the F

| Configuration File | Restart Required | Read/Write Permission |
|---|---|---|
| /sg/sip_hosts | N | |
| /sg/tid-app | N | |
| /sg/sip.cfg | Y | |
| /sg/tls/tls_CN | N | |
| /sg/tls/http_spid_cfg | Y | |
| /sg/sys_mem2 | Y | |

You can get to the advanced parameters by going to: System -> Advanced -> Advanced Parameters.

If any of these Advanced Parameters is not display please contact Sansay Support.
Advanced Parameters needs to be updated on Active and also Standby server.

# VSXI CONFIGURATION – ADV PARAMETERS

## /sg/tid-app

This Advanced parameter file is used to enable specific TID settings. For Microsoft Teams configuration the following entries are required.

```
# Enable Permanent OPTIONS  Polls to MS Teams
Options: IP=sip.pstnhub.microsoft.com PORT=5061 SP_ID=X
Options: IP=sip2.pstnhub.microsoft.com PORT=5061 SP_ID=X
Options: IP=sip3.pstnhub.microsoft.com PORT=5061 SP_ID=X
#Enable Microsoft Mode for TID
Microsoft_Mode: TID=2000
Microsoft_Mode: TID=2001
#Set 180Rinback for MS teams TID
180Ringback: TID=2000 MODE=180 MAX=10 TERM
180Ringback: TID=2001 MODE=180 MAX=10 TERM
```

Where:

TID 2000 & 2001 is your MS Teams TID facing Microsoft SIP Proxy.

X is the Service Port Id for the TLS Service Port.

# VSXI CONFIGURATION – ADV PARAMETERS

## /sg/sip.cfg

```
# Apply SMC 552 to OPTION poll for MS teams
168,d,552
#Ringback for transfer
183,d,1
```

Where 552 is the SMC profile for MS Teams Options Polls.

## /sg/tls/tls_CN

```
IP=52.114.148.0 CN=sip.pstnhub.microsoft.com
IP=52.114.132.46 CN=sip.pstnhub.microsoft.com
IP=52.114.75.24 CN=sip.pstnhub.microsoft.com
IP=52.114.76.76 CN=sip.pstnhub.microsoft.com
IP=52.114.7.24 CN=sip.pstnhub.microsoft.com
IP=52.114.14.70 CN=sip.pstnhub.microsoft.com
IP=52.114.16.74 CN=sip.pstnhub.microsoft.com
IP=52.114.20.29 CN=sip.pstnhub.microsoft.com
IP=52.114.36.156 CN=sip.pstnhub.microsoft.com
IP=52.114.32.169 CN=sip.pstnhub.microsoft.com
```

# VSXI CONFIGURATION – ADV PARAMETERS

## /sg/tls/http_spid_cfg

```
#Enable RFS
SPID=999 Type=FS
```

Where 999 is the Service Port Id for the RFS-In.

## /sg/sys_mem2

```
[SSM]
IceBlocks = 1000
```

# VSXI CONFIGURATION – MST3 config

If you are using MST3 (External Media Server), you need to make sure the following advanced parameter enabled:

/sg/sys_mem2

```
[MHP]
UserPlaneSSE      = 1
```

**Important information:**
MS Teams blind transfer action requires the SBC to generate local RBT during ringing phase while connecting to the transfer target. This feature (Local RBT generation) requires the presence of transcoding capability and license. Without transcoding, transfer will complete but no RBT will be heard when the calls connects to the transfer target.