Configuring Patton SmartNode eSBC with Microsoft Teams Direct Routing without Media Bypass

Version 2.1

Patton Electronics Co. | www.patton.com
7622 Rickenbacker Drive, Gaithersburg, MD 20879, USA
tel: +1 301-975-1000 | fax: +1 301-869-9293
Email (sales): sales@patton.com
Email (support): support@patton.com

Table of contents

Revision history

Document version	Editor	Description of changes	Date of revision
1.0	Bojan Radovic	Initial document version	15.12.2020
1.1	Bojan Radovic	Added configuration template for topology with IPPBX	05.01.2021
1.2	Bojan Radovic	Minor changes in chapter 1.1	18.01.2021
1.3	Bojan Radovic	Correction chap 1.3 & config. template	03.02.2021
1.4	Bojan Radovic	Completed chapter with TLS certificate handling	05.02.2021
1.5	Bojan Radovic	Added spoofed VIA-Header in the configuration templates	01.03.2021
1.6	Bojan Radovic	Completed chapter with TLS certificate handling; History-Info header added to the configuration templates.	17.03.2021
1.7	Bojan Radovic	Updated the list of IP addresses resolved by the FQDNs of Microsoft Updated licensing chapter	04.05.2021
1.8	Bojan Radovic	Added dedicated TLS profile for Teams (instead of using the default one) Modified Mapping Tables to comply with the specific Teams handling of privacy & anonymous calls	25.05.2021
1.9	Bojan Radovic	Updated PowerShell chapter after EOL of SfB Online Connector	11.06.2021
2.0	Bojan Radovic	Updated ACL lists with new subnets of Microsoft Updated Location Service domain names (for anonymous call from Teams)	23.08.2021
2.1	Bojan Radovic	Added chapter “4.4.1 Web Wizards for Teams” Session refresh method updated on all SIP interfaces	06.04.2022

1 Introduction

This Configuration Guide is a technical description intended to IT Administrators, Network and VoIP Engineers who need to connect Patton's Session Border Controllers to Microsoft Teams Direct Routing.

More precisely, it provides the configuration steps to interconnect Patton SmartNode eSBC's (Enterprise Session Border Controllers) to Microsoft Teams Direct Routing without Media-Bypass.

1.1 About MS Teams Direct Routing

Direct Routing allows customers with existing Enterprise Telephony infrastructure (PBX / IPPBX) to keep their preferred telecom provider to enable their users to setup and receive calls in Teams.

If Teams and Phone System is available in your country, you can start planning and deploying Direct Routing in your organization. Direct Routing allows you to setup and receive phone calls through your existing PBX system and Teams.

By integrating both systems through Direct Routing, the existing telephony user experience is kept and extended through Teams. It allows to combine the high level of internal business telephony features of a PBX, like group calls, Call Center / ACD, support of legacy user lines, least cost routing etc. with the UCC-features provided by Teams like Instant Messaging & Presence, File and Desktop Sharing, Video Conferencing etc.

1.2 About Patton SBC Product Series

SmartNode 5500 Series Enterprise Session Border Controllers (eSBC) constitute Patton's main SBC product line addressing small and medium enterprises.

The SN5500 series integrate an enterprise router to a SIP trunk or hosted PBX service. Depending on model, it supports up to 200 SIP to SIP calls or up to 100 Teams calls, 16 out of which can be transcoded - for reliable remote or branch office connectivity and enhanced All-IP carrier services. The SN5500 acts as an eSBC, access router, probe and QoS CPE all-in-one device. It can also undertake network assessment and monitoring at the customer premise to prevent, reduce and resolve network and voice quality problems.

Whether used as eSBC or IP router, the SmartNode 5500 provides excellent VoIP, IP QoS and security features for seamless network integration. Thanks to the built-in SIP back-to-back user agent, it resolves technology evolution related problems by normalizing SIP traffic from different vendor implementations. In addition, enhanced security is given to the enterprise thanks to various features protecting the LAN infrastructure. Number manipulation and call routing options belong to the basic capabilities offered by every Patton eSBC.

The following table is a general overview of the whole SBC product line of Patton, in which the Teams certified models are highlighted correspondingly.

eSBC	vSN	SN500	SN5300	SN5480	SN5490	SN5500	SN5530	SN5540	SN5550	SN5570	SN5600	SN10500
Product Photo												
Embedded Software	Trinity™	Trinity™	Trinity™	SmartWare™ or Trinity™	SmartWare™ or Trinity™	Trinity™	Trinity™	Trinity™	Trinity™	Trinity™	Trinity™	SmartMedia™
Telephony Interfaces	N/A	N/A	N/A	N/A	N/A	N/A	2, 4 or 8 BRI	2, 4 or 8 FXS/FXO	BRI with FXS/FXO	1 or 2 PRI	N/A	N/A
SIP Sessions	1 to 1,000's	4 to 30	4 to 60	Up to 80	Up to 80	4 to 200	4 to 200	4 to 200	4 to 200	4 to 200	4 to 1,000	5,000
Transcoded Calls	N/A	N/A	N/A	Up to 64	Up to 64	Up to 16	Up to 8	Up to 4	Up to 4	Up to 15	N/A	2,744
IP router IP Routing, QoS, VPN, etc.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A
Number of Ethernet Ports	HW dependent	2 10/100/1000	4 10/100	2 10/100/1000	2 10/100/1000	2 10/100/1000	2 10/100/1000	2 10/100/1000	2 10/100/1000	2 10/100/1000	2 10/100/1000	Up to 6 10/100/1000
Transcoding	Roadmap	N/A		✓	✓	✓	✓	✓	✓	✓	N/A	✓
WAN Access	N/A	N/A	G.SHDSL.bis (ATM or EFM)		Fiber G.SHDSL EFM X.21	G.SHDSL EFM&ATM, ADSL-VDSL	VDSL/ADSL G.SHDSL.bis	VDSL/ADSL G.SHDSL.bis		VDSL/ADSL G.SHDSL.bis	N/A	N/A

For a general product line overview of Patton Session Border Controllers, please visit the Patton SmartNode webpage:

https://www.patton.com/products/voip-comparison.asp

then click on **eSBC**.

1.3 Validated Patton eSBC Version

Microsoft has successfully performed the certification tests with the following Patton eSBC:

SmartNode 5501/8P, Software Version Trinity 3.18.1

Additionally Patton conducted internal validation tests and reached the same interoperability level with Teams Direct Routing for following eSBC series:

eSBC Model	**Type**	**SW version tested with success**	**Recommended SW version**
SN5501/8P SN5501/16P	IP-IP SBC	Trinity 3.18.1	3.19.x and higher
SN5531	SBC with ISDN BRI GW	Trinity 3.18.1	3.19.x and higher
SN5541	SBC with FXS/FXO GW	Trinity 3.18.1	3.19.x and higher
SN5551	SBC with ISDN BRI/FXS/FXO GW	Trinity 3.18.1	3.19.x and higher
SN5571	SBC + PRI GW	Trinity 3.18.1	3.19.x and higher

2 Tested SBC Topologies

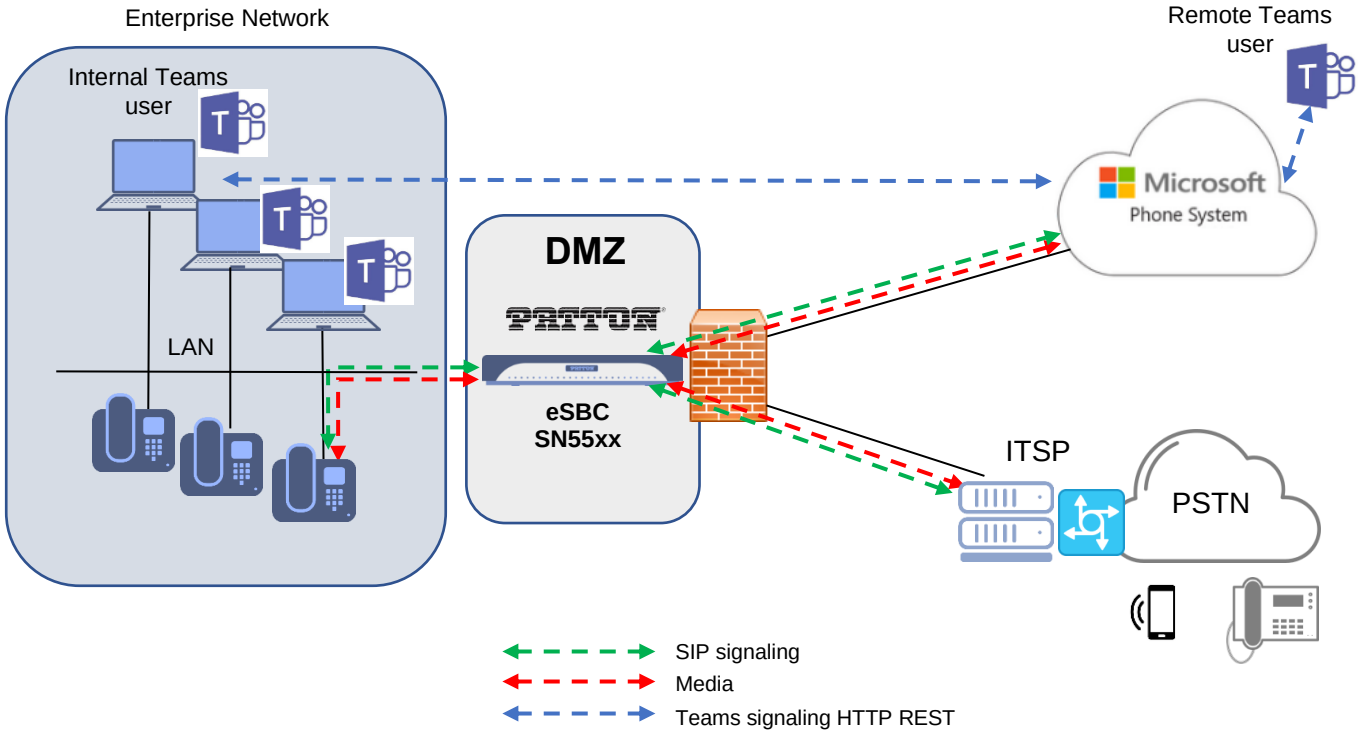
2.1 Direct Routing without IPPBX

In this connection topology the connections to Teams Direct Routing and the SIP-Trunk to the PSTN network are both located on the public / WAN side of the SBC, whereas on the Enterprise network side there is no IPPBX, but only user end devices.

Following connection entities are shown in the figure:

- Enterprise network consisting of SIP devices, Teams clients and softphones. ISDN or analog devices may also be considered in case of use of Patton eSBC with Gateway functionality (not represented in this figure).
- Microsoft Teams Direct Routing Interface on the WAN
- SIP trunk from a third-party VoIP provider, which is located on the WAN in this topology

Topology 1 - without IPPBX



2.2 Direct Routing with IPPBX

In this connection topology the connection to Teams Direct Routing is located on the public / WAN side of the SBC, the IPPBX on the LAN side, whereas the SIP-Trunk is connected either through the SBC WAN interface like in the previous topology or through the IPPBX on LAN.

These two variants have to be considered separately because the call flows are slightly different, which also slightly impacts the internal call routing of the eSBC.

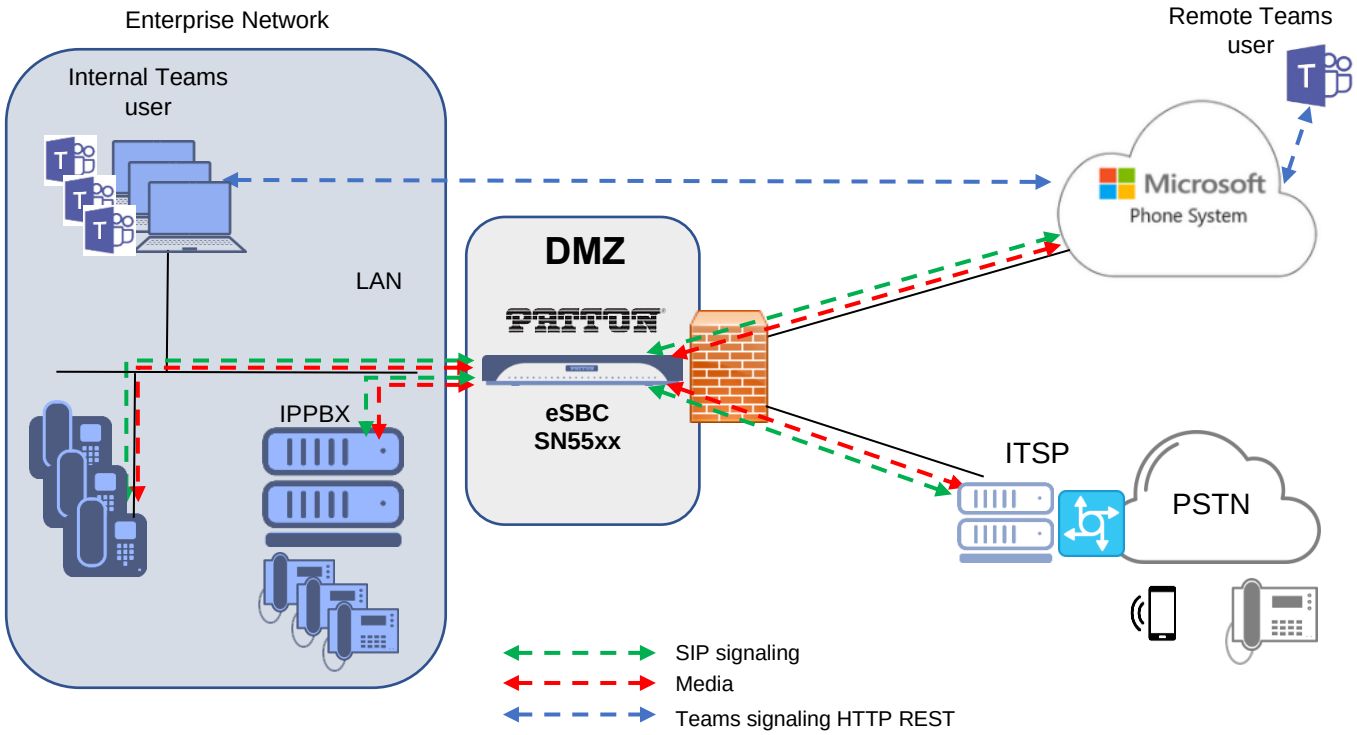
We present both variants in the following two subsections.

2.2.1SIP-Trunk to PSTN over SBC (WAN)

Following connection entities are shown in the figure:

- Enterprise network consisting of an IPPBX, proprietary phones, SIP devices, Teams clients and softphones. ISDN or analog devices may also be considered in case of use of Patton eSBC with Gateway functionality (not represented in this figure).
- Microsoft Teams Direct Routing Interface on the WAN
- SIP trunk from a third-party VoIP provider, which is located on the WAN side of the SBC in this topology

Topology 2 - IPPBX & SIP-Trunk over SBC (WAN)



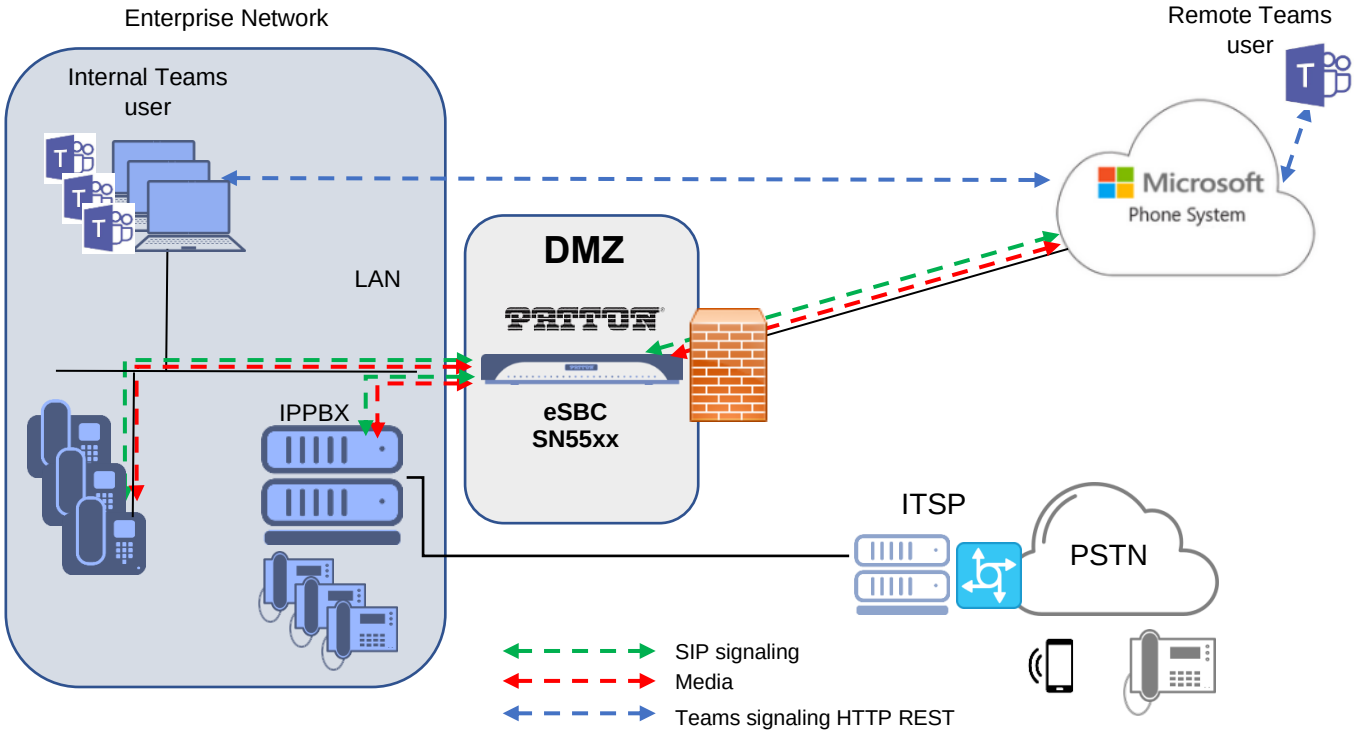
2.2.2 SIP-Trunk to PSTN over IPPBX (LAN)

Following connection entities are shown in the figure:

- Enterprise network consisting of an IPPBX, proprietary phones, SIP devices, Teams clients and softphones. ISDN or analog devices may also be considered in case of use of Patton eSBC with Gateway functionality (not represented in this figure).
- Microsoft Teams Direct Routing Interface on the WAN

- SIP trunk from a third-party VoIP provider, which is located on the LAN and connected through the IPPBX

Topology 3 - SIP-Trunk over IPPBX (over LAN)



3 Planning and configuring Teams Direct Routing

3.1 Planning Direct Routing

Before setting up MS Teams Direct Routing with Patton SBC, planning your deployment of Direct Routing is key to a successful implementation.

All the planning tasks recommended by Microsoft shall be implemented as described in their online documentation:

https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-landing-page

https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-plan

Main tasks summary:

- Infrastructure requirements
- Licensing and other requirements
- SBC domain names
- Public trusted certificate for the SBC
- SIP Signaling: FQDNs

We have briefly described these tasks below. For more details, please read the documentation on the mentioned website of Microsoft.

3.1.1 Infrastructure requirements

- Configured PSTN connectivity through telephony trunks on Patton SBC. Those trunks can be SIP or TDM (ISDN or analog) depending on your provider's access type.
- Ensure that you have a custom domain on your Microsoft 365 or Office 365 organization that you use to home your Microsoft Teams users.
- A public IP address shall be assigned to the SBC.
- A Fully Qualified Domain Name (FQDN) must be assigned to the SBC, where the domain portion of the FQDN is one of the registered domains in your Microsoft 365 or Office 365 organization.
- A public DNS entry must exist, which maps the SBC FQDN to its public IP Address.
- A public trusted certificate must be installed on the SBC. It is used for the mandatory encrypted communication over Direct Routing.
- The connection points for Direct Routing are the following three FQDNs:
  `sip.pstnhub.microsoft.com` – Global FQDN, must be tried first.
  `sip2.pstnhub.microsoft.com` – Secondary FQDN, geographically maps to the second priority region.
  `sip3.pstnhub.microsoft.com` – Tertiary FQDN, geographically maps to the third priority region.

3.1.2 Licensing and other requirements

On Microsoft side, your organization needs to acquire the best suitable Microsoft Office licenses for the planned size of your Teams user group.

If you are a **small or medium-sized business** (less than 300 users), you need to acquire one of the following licenses to get Teams Direct Routing:

- Microsoft 365 Business plan and Microsoft 365 Business Voice without a Calling Plan (Direct Routing)
  or
- Enterprise E1 or E3 plan and Microsoft 365 Business Voice without a Calling Plan (Direct Routing)
  or
- Enterprise E1 or E3 plan and add voice features individually
  or
- Enterprise E5 plan, which includes voice features

If you are a **large business or enterprise organization** (more than 300 users), you need to acquire one of the following licenses to get Teams Direct Routing:

- Enterprise E1 or E3 plan and add voice features individually
  or
- Enterprise E5 plan, which includes voice features.

Note that the Business Voice license is sometimes referred to as Phone System license, as the Phone System is the central part of it.

For test environments and trials only, some cheaper Microsoft licenses might be useful, like MS 365 F1 + Microsoft 365 Business Voice without a Calling Plan (Direct Routing). We advise to acquire this license combination only for test or Proof of Concept purposes, as it is intended for users without a dedicated device.

Another option for test purpose is an E3 trial or an E5 trial license.

3.2 Configuring Direct Routing

To complete the steps explained in this article, administrators need some familiarity with PowerShell cmdlets.

We strongly recommend to consult the corresponding documentation and the available Admin training for Teams.

Configuring Direct Routing:
https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-configure

Admin trainings landing page:
https://docs.microsoft.com/en-us/MicrosoftTeams/itadmin-readiness#technical-training

Admin training: “Planning for Direct Routing in Microsoft Teams”:
https://youtu.be/nb_fV9aG_JY

Admin training: “Configuring and Managing Direct Routing in Microsoft Teams”: https://youtu.be/zXDNLwmC1vM

3.2.1Configure Direct Routing using Windows PowerShell

This chapter has been updated in the version 1.9 of the present configuration guide according to the End-of-Life of the former Skype for Business Online Connector. Since February 2021, the Powershell module MicrosoftTeams is to be used instead of the former / phased-out SkypeOnlineConnector module.

If you use PowerShell for the first time for Teams Direct Routing configuration, then you need to proceed to these initial settings, otherwise you will notice that the commands are unknown.

One time procedure as PowerShell administrator:

Install the Teams PowerShell module by using the following PowerShell command as administrator:

```
Install-Module MicrosoftTeams
```

Then exit and re-open PowerShell as administrator.

To access the module, start a Windows PowerShell session as administrator, then run the following set of commands by replacing `user.name` by your own user name in and `yourdomainname.com` by your organization’s domain name. Here you must provide a Microsoft account or organizational ID credentials. If multi-factor authentication is enabled for your credentials, you must log in using the interactive option.

```
#Import module
Import-Module MicrosoftTeams
#Connect Teams
$userCredential = Get-Credential -Credential user.name@yourdomainname.com
Connect-MicrosoftTeams -Credential $userCredential
```

As this command set is to be executed at each PowerShell session for Direct Routing configuration and administration, you can avoid it by creating a batch file the following way from a PowerShell session:

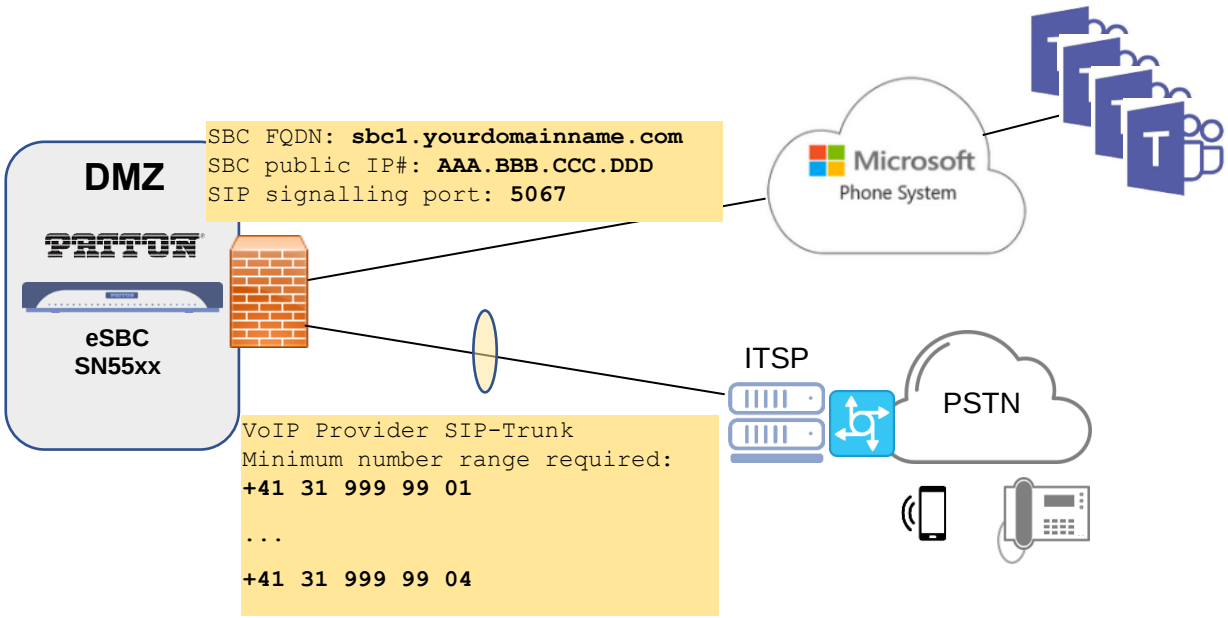
```
notepad.exe $profile
```

(path: C:\Users\<username>\Documents\WindowsPowerShell)

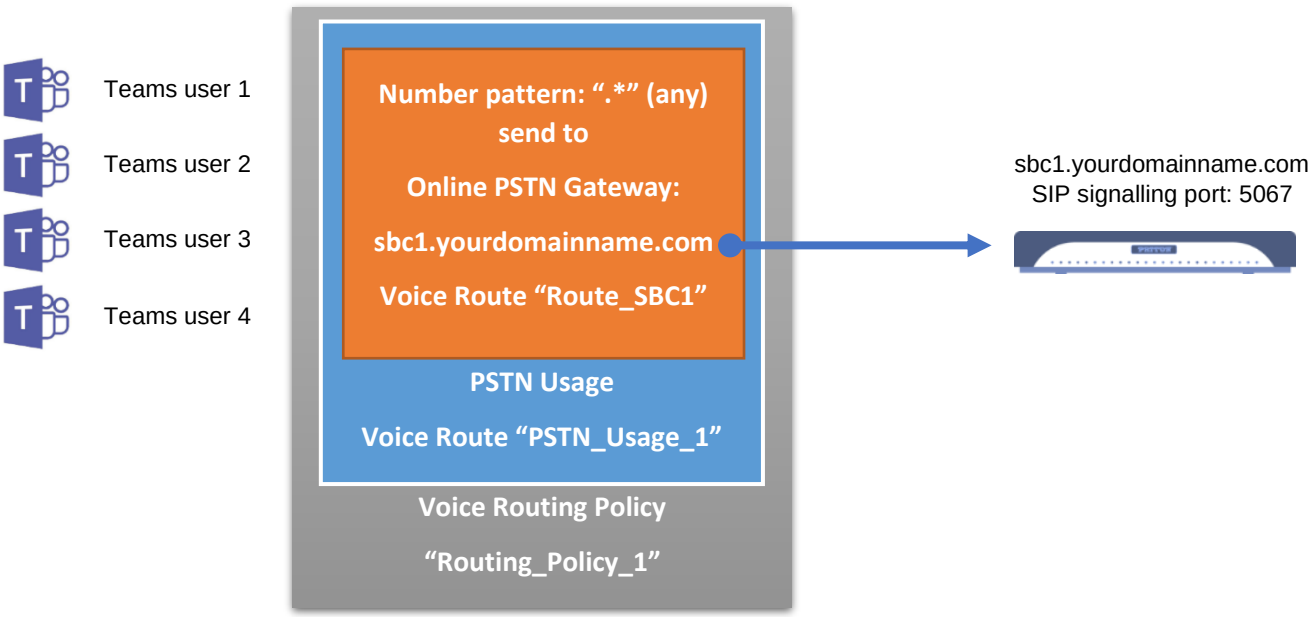
Then copy & paste the command set listed above to the batch file and save it. This profile will be called at each future start of a new PowerShell session.

For this configuration let’s consider the first simple topology without IPPBX with following dummy FQDNs, SIP data and phone numbers assigned to four test Teams users. We do not represent the LAN side here, as it is not relevant at this configuration step.

Teams user name	Assigned PSTN phone number
msteamsuser1@yourdomainname.com	**+41 31 999 99 01**
msteamsuser2@yourdomainname.com	**+41 31 999 99 02**
msteamsuser3@yourdomainname.com	**+41 31 999 99 03**
msteamsuser4@yourdomainname.com	**+41 31 999 99 04**



We will use the following example of voice routing configuration in MS Phone System:



Configuration cmdlets

```
New-CsOnlinePSTNGateway -Fqdn sbc1.yourdomainname.com -SipSignallingPort 5067 -
ForwardCallHistory $True -MaxConcurrentSessions 100 -Enabled $True

Set-CsOnlinePstnUsage -Identity Global -usage @{Add="PSTN_Usage_1"}

New-CsOnlineVoiceRoute -Identity "Route_SBC1" -NumberPattern ".*" -
OnlinePstnGatewayList sbc1.yourdomainname.com -Priority 1 -OnlinePstnUsages
"PSTN_Usage_1"

New-CsOnlineVoiceRoutingPolicy "Routing_Policy_1" -OnlinePstnUsages "PSTN_Usage_1"

Set-CsUser -Identity "msteamsuser1@yourdomainname.com" -OnPremLineURI tel:+41319999901
-EnterpriseVoiceEnabled $true -HostedVoiceMail $true

Set-CsUser -Identity "msteamsuser2@yourdomainname.com" -OnPremLineURI tel:+41319999902
-EnterpriseVoiceEnabled $true -HostedVoiceMail $true

Set-CsUser -Identity "msteamsuser3@yourdomainname.com" -OnPremLineURI tel:+41319999903
-EnterpriseVoiceEnabled $true -HostedVoiceMail $true

Set-CsUser -Identity "msteamsuser4@yourdomainname.com" -OnPremLineURI tel:+41319999904
-EnterpriseVoiceEnabled $true -HostedVoiceMail $true

Grant-CsOnlineVoiceRoutingPolicy -Identity "msteamsuser1@yourdomainname.com"  -
PolicyName "Routing_Policy_1"

Grant-CsOnlineVoiceRoutingPolicy -Identity "msteamsuser2@yourdomainname.com"  -
PolicyName "Routing_Policy_1"

Grant-CsOnlineVoiceRoutingPolicy -Identity "msteamsuser3@yourdomainname.com"  -
PolicyName "Routing_Policy_1"

Grant-CsOnlineVoiceRoutingPolicy -Identity "msteamsuser4@yourdomainname.com"  -
PolicyName "Routing_Policy_1"
```

Get-commands / configuration check:

```
Get-CsOnlinePSTNGateway
Get-CsOnlinePstnUsage
Get-CsOnlineVoiceRoute
Get-CsOnlineVoiceRoutingPolicy

Get-CsUserPolicyAssignment -Identity msteamsuser1@yourdomainname.com
Get-CsUserPolicyAssignment -Identity msteamsuser2@yourdomainname.com
Get-CsUserPolicyAssignment -Identity msteamsuser3@yourdomainname.com
Get-CsUserPolicyAssignment -Identity msteamsuser4@yourdomainname.com

Get-CsOnlineUser -Identity msteams* | Format-List Alias, UserPrincipalName,
OnPremLineURI, EnterpriseVoiceEnabled, HostedVoiceMail, OnlineVoiceRoutingPolicy,
CallingLineIdentity
```

Output example of such format of Get-CsOnlineUser command:

```
Alias                     : msteamsuser4
UserPrincipalName         : msteamsuser4@companyname.com
OnPremLineURI             : tel:+41319999904
EnterpriseVoiceEnabled    : True
HostedVoiceMail           : True
OnlineVoiceRoutingPolicy  : Routing_Policy_1
CallingLineIdentity       :

Alias                     : msteamsuser3
UserPrincipalName         : msteamsuser3@companyname.com
OnPremLineURI             : tel:+41319999903
EnterpriseVoiceEnabled    : True
HostedVoiceMail           : True
OnlineVoiceRoutingPolicy  : Routing_Policy_1
CallingLineIdentity       :

Alias                     : msteamsuser2
UserPrincipalName         : msteamsuser2@companyname.com
OnPremLineURI             : tel:+41319999902
```

```
EnterpriseVoiceEnabled   : True
HostedVoiceMail          : True
OnlineVoiceRoutingPolicy : Routing_Policy_1
CallingLineIdentity      :

Alias                    : msteamsuser1
UserPrincipalName        : msteamsuser1@companyname.com
OnPremLineURI            : tel:+41319999901
EnterpriseVoiceEnabled   : True
HostedVoiceMail          : True
OnlineVoiceRoutingPolicy : Routing_Policy_1
CallingLineIdentity      :
```

4 Configuring the SBC

SmartNode 5501 front and rear view:

Main tasks summary

- Minimum Software requirements for the SN55xx eSBC
- Software licenses
- TLS Certificate
- Public IP address

4.1 Minimum Software requirements

As first task, we recommend to update the embedded Software on your Patton SmartNode eSBC to version 3.19.x

- Patton Software Upgrade Portal: https://www.patton.com/support/upgrades/
- Select your SmartNode eSBC model, for example SN5501/8P or SN5501/16P

The latest version is always highly recommended, in order to be up-to-date with the last bugfixes and SIP features.

4.2 Software licenses

For the configuration of Teams Direct Routing on Patton eSBC following SW license shall be acquired, additionally to the licenses installed by default.

Catalog #: Description:

TSW-MST HW based license for MS Teams SBC, including TLS & SRTP

Or if you use Patton Cloud license server

CBFL-MST Yearly Cloud based license for MS Teams SBC, incl. TLS & SRTP

This license enables Teams Direct Routing and includes TLS as well as SRTP media encryption.

Additional SIP session licenses may be required if the amount of the pre-installed SIP sessions are not enough, depending on the purchased SBC model.

Example: SN5501/16P has 16 built-in SIP Calls (all transcoded). If you require up to 30 SIP calls for your customer setup, you have to upgrade the device by adding 14 additional **SIP licenses** (reference code **SNSW-1B**).

For further details please contact your Patton distributor or Patton Sales representative.

4.3 TLS Certificate

The main requirements of Microsoft regarding the TLS Certificate on SBC are the following:

- You should request the certificate for the SBC by generating a certification signing request (CSR). Self-signed certificates are not accepted.
- The certificate needs to have the SBC FQDN as the common name (CN) in the subject field.
- The certificate should be issued directly from a certification authority, not from an intermediate provider.
- Alternatively, Direct Routing supports a wildcard in the Subject Alternative Name (SAN), and the wildcard needs to conform to standard RFC HTTP Over TLS.

For general information and planning of this task, we recommend you to read the chapter *Public-Key Infrastructure (PKI)* of the *Command Line Reference Guide* for Patton SBC devices. It provides an overview on how to set up the public-key infrastructure on a Patton device. PKI deals with the creation, management and deployment of keys and certificates, which is an intricate task.

The following subchapters provide the detailed procedure to enroll a CA-signed TLS certificate on Patton eSBC devices.

4.3.1Generate a private/public key pair on the device.

Use the following CLI command on the SBC by adapting the key filename accordingly:

```
sbc1(cfg)#generate pki:private-key/sbc1.yourdomainname.com.key key-length 2048
```

After private key generation, a related public key is automatically created.

Note that the private key content can never be displayed for security reasons, neither through CLI nor through the Web GUI.

4.3.2Generate a certificate request

Use the following CLI command on the SBC by changing the field contents according to your organization context. The values below are just dummy examples for a supposed organization located in Switzerland:

```
sbc1(cfg)#generate pki:certificate-request/request1 private-key
pki:private-key/sbc1.yourdomainname.com.key country CH state Bern
locality Bern organization Your-Companyname organization-unit VOIP
common-name sbc1.yourdomainname.com
```

4.3.3Export the request on the SBC

```
sbc1(cfg)#export pki:certificate-request/request1
```

```
-----BEGIN CERTIFICATE REQUEST-----
MIICpTCCAY0CAQAwYDELMAkGA1UEBhMCQ0gxDTALBgNVBAgMBEJlcm4xDTALBgNV
NF9cuDx4qqsSIBIJ9Yv1C2X6T0WjTyOHQDICHAr58PTRT+MzR98LJkPMFX0bBoQd
...
...
...
y3f71W3oPz602akU48nRPPPrToFm4Z1zULiCrGGEhaMQK2bPMxoTt//HC/jCyNe+
wEPaIWE1LmPz
-----END CERTIFICATE REQUEST-----
```

Either copy the printout of the export command including the BEGIN / END commands from the terminal or execute the following command to upload the request to a TFTP server:

```
#copy pki:certificate-request/request1 tftp://<server>/request1
```

You can also use the Web GUI to download the certificate request.

Then send it to the CA for approvement and signing. The certificate needs to be generated by one of the root CA listed in the online documentation for Microsoft Teams planning:

https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-plan#public-trusted-certificate-for-the-sbc

4.3.4Approvement and signing by the CA

After the CA approves the certificate request, it signs it with its own private key and returns the issued signed certificate in one of the most usual file extension formats *.cer, *.crt, .pem, .p12 etc.

Example: `sbc1.yourdomainname.com.crt`

4.3.5Import the signed certificate to Patton eSBC

At this step, you have to import the signed certificate issued by the CA to the Patton device. If the device certificate is signed by the root CA directly, you only have to import the device certificate here without intermediate certificates. If in contrary the device certificate is signed by an intermediary Certificate Authority, then an intermediate certificate, which identifies the intermediary Certificate Authority between the root certificate and the personal certificate, has also to be imported. It is recommended to issue the certificate directly from a certification authority, not from an intermediate provider.

Copy the device certificate from your TFTP server to the Patton device's persistent memory by executing the following command:

```
sbc1(cfg)#copy tftp://<ip-address>/sbc1.yourdomainname.com.crt
pki:certificate/sbc1.yourdomainname.com.crt
```

or use the Web GUI to upload it to the SBC.

After importing the TLS certificate, you have to link the private key and the issued certificate to the TLS profile that you are going to use in your SIP Gateway.

Link the previously generated private key to the TLS profile used for Teams:

```
#(cfg)#profile tls PF_TLS_TEAMS

#private-key pki:private-key/sbc1.yourdomainname.com.key
```

Import the signed certificate by using the CLI command own-certificate:

```
#own-certificate pki:certificate/sbc1.yourdomainname.com.crt
```

If any intermediate certificate has been used to sign our own certificate, import it as well by using the same own-certificate CLI command):

```
node(pf-tls)[DEFAULT]#own-certificate 2 pki:certificate/CERT_OF_MY_CA
```

If another root certificate than one of the default installed ones on the Patton device was used for signing the TLS certificate, then you also have to import and link it to the profile with the command:

```
trusted-certificate pki:trusted-certificate/ROOT
```

In our example, we use a dedicated TLS profile on the SBC, that we call here PF_TLS_TEAMS, whose content is the following after the steps above including the certificate import:

```
profile tls PF_TLS_TEAMS
  no protocol tls-v1.0
  no protocol tls-v1.1
  compression
  authentication incoming
  authentication outgoing
  private-key pki:private-key/sbc1.yourdomainname.com.key
  own-certificate 1 pki:certificate/sbc1.yourdomainname.com.crt
  own-certificate 2 pki:certificate/CA
  trusted-certificate pki:trusted-certificate/ROOT
  diffie-hellman-parameters pki:diffie-hellman-parameters/DEFAULT-4096
  require certificate-type server
```

The TLS profile is also included and commented in the attached complete SBC configuration samples at the end of this guide.

4.4 SmartNode 5501 Configuration

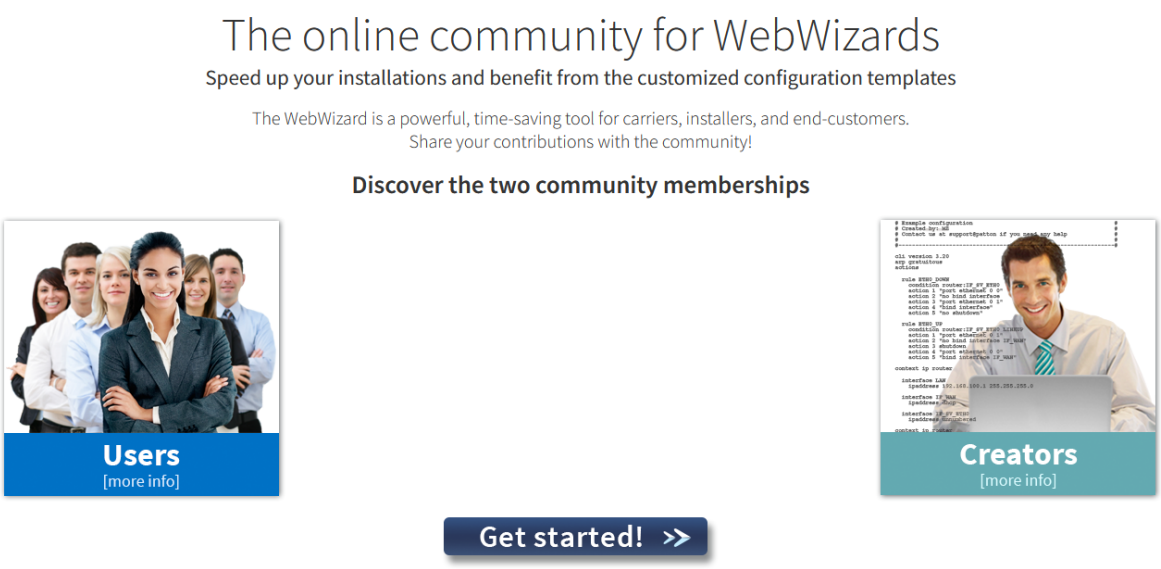
4.4.1Web Wizards for Teams

Although we provide the configuration samples for the two mentioned topologies in the two next subchapters, we strongly recommend using Patton Web Wizards as configuration templates in order to generate your initial eSBC configuration for Teams Direct Routing, because these are regularly updated through the last changes and

corrections. They also allow you to easily manipulate and edit the configuration file, because they include all the fix parts listed in the attached samples further below.

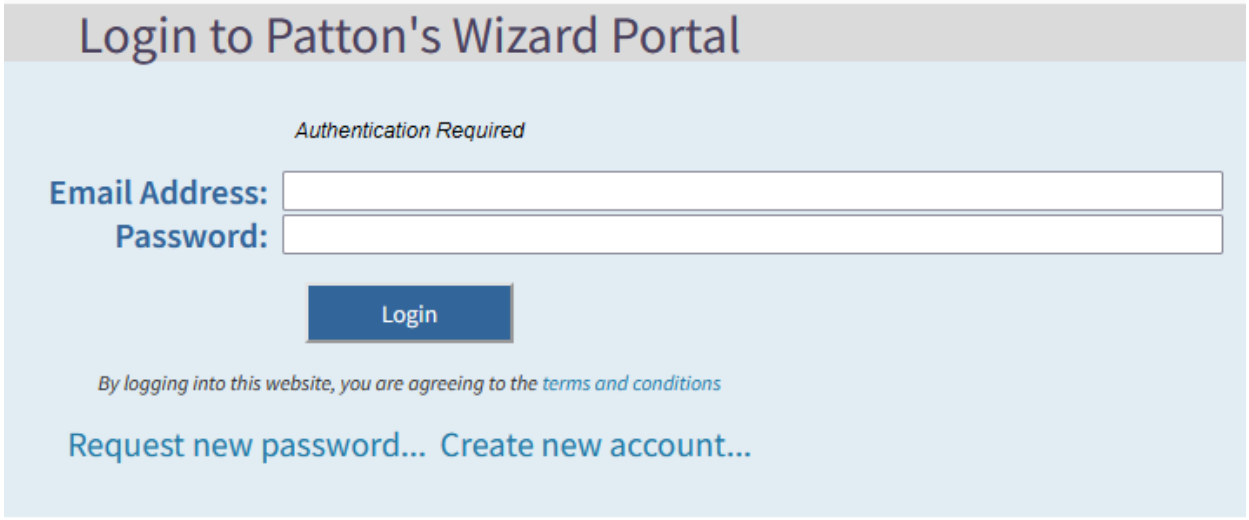
How to proceed:

Link: https://www.patton.com/wizard/

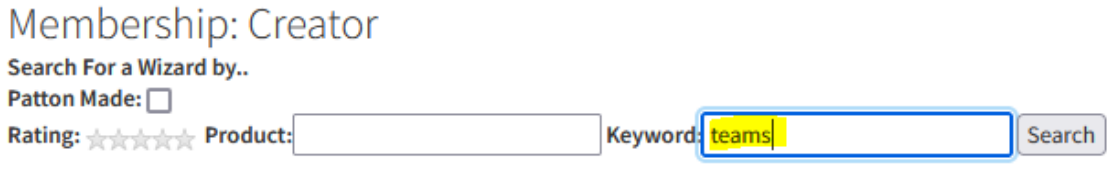


Click on “Get started! >>”

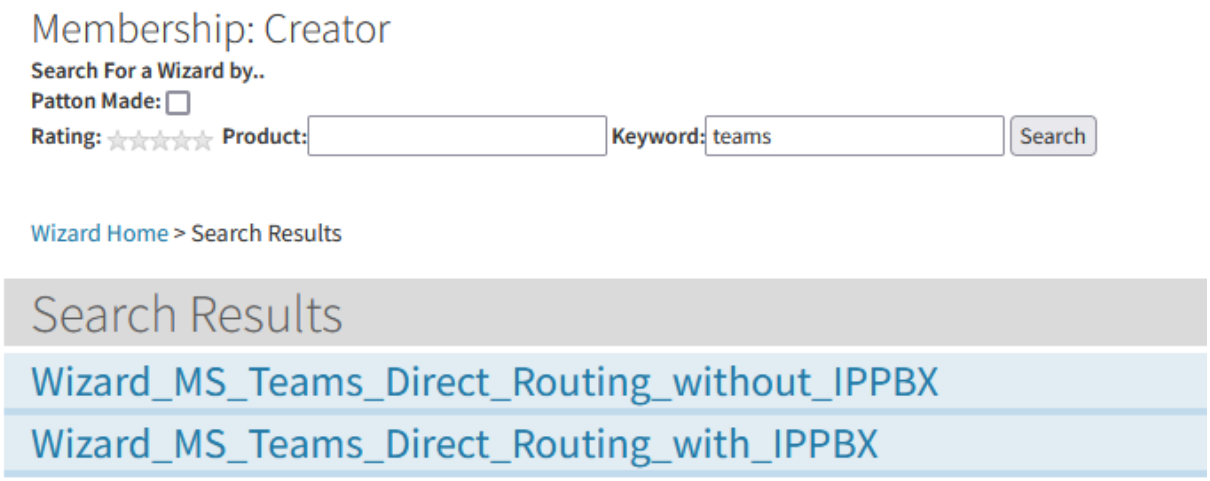
A Patton Login is required for the access. If not already available, you can create a new account.



On the main Web Wizard page start a search by keyword ‘teams’:



The search result will provide you the two corresponding Web Wizards:



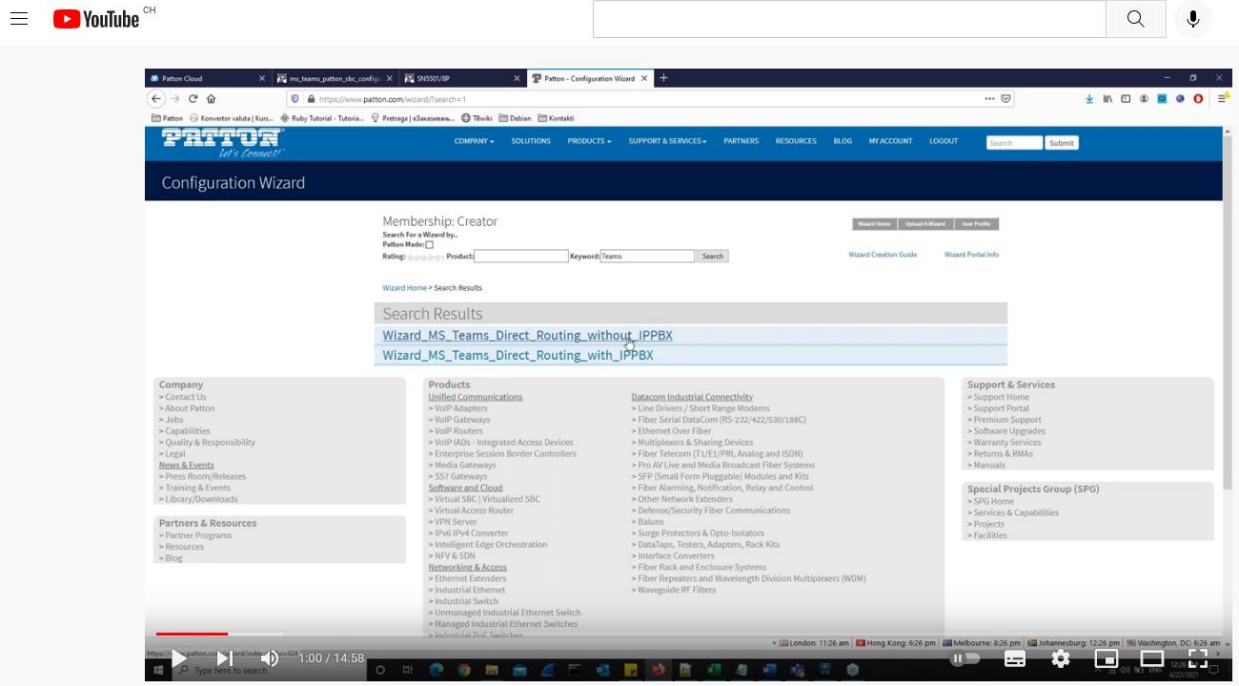
Choose the matching one for your project, for example for the use case without IPPBX, and start it by clicking on “Run Wizard”.

Then fill out all the requested fiels by the variables parameters of your setup, like admin password, IP addresses, SIP user names/passwords etc.

Once you have filled out all the required fields, a Preview option allows you to display the whole eSBC configuration generated by the tool.

For a detailed step-by-step description of the generation of your initial eSBC configuration, we suggest you the useful online video tutorial “SmartNode SBC Configuration for Microsoft Teams (updated video)” on Youtube:

https://youtu.be/0nUDaq73Os8



4.4.2Configuration sample for topology 1

This is the SN5501 SBC configuration file sample for the topology 1 described before, i.e. **Teams Direct Routing without IPPBX**. The SIP-Trunk towards PSTN is realized with the Swiss VoIP provider Peoplefone. Note that the SIP interface configuration part for the VoIP provider side can vary considerably depending on the provider's technical specification for the SIP-Trunk.

Configuration parts highlighted in green: fix parts mandatory for Teams Direct Routing

Configuration parts highlighted in yellow: variable / project specific parts, that must be set to values that depend on the environment (IP addresses, domain names, SIP Gateway names containing provider name, routing/mapping table names with provider name …)

Not highlighted parts: recommended to leave as displayed but may be changed to other values depending on your needs.

Text boxes on the right side contain comments related to the configuration.

```
cli version 4.00
superuser superuser password XXXXXXX
system hostname sbc1.yourdomainname.com
system description "SBC connected to MS Teams"
system location "Patton Inalp - Bern CH"
clock local default-offset +01:00
clock local dst-rule SUMMERTIME +1:00 from mar last
sunday 02:00 2019 until oct last sunday 03:00 2036

profile aaa DEFAULT
  method 1 nodems continue-on-reject
  method 2 local
  method 3 none

console
  use profile aaa DEFAULT
```

Set your own superuser name and password.

Depending on the local time zone, set the corresponding default offset to UTC, and additionally set the Daylight Saving Time (DST) if necessary in your time zone. The example on the left is correct for CET time zone with DST.

```
telnet-server
  use profile aaa DEFAULT
  shutdown

ssh-server
  use profile aaa DEFAULT
  no shutdown

snmp-server
  shutdown

web-server
  no protocol http
  protocol https port 443
  use profile aaa DEFAULT
  no shutdown

ntp
  server 0.patton.pool.ntp.org
  server 1.patton.pool.ntp.org
  server 2.patton.pool.ntp.org
  server 3.patton.pool.ntp.org
  no shutdown

profile napt NAPT_WAN

profile acl ACL_WAN_IN_DENY
  permit 1 protocol tcp src-ip 52.112.0.0/14 dest-port 5061
  permit 2 protocol tcp src-ip 52.120.0.0/14 dest-port 5061
  permit 3 src-ip XXX.XXX.XXX.XXX/XX

profile acl ACL_WAN_PROTOCOLS
  permit 1 protocol udp dest-port 53,123,5060,5061
  permit 2 protocol tcp dest-port 53,443,5060,5061
  permit 3 protocol icmp

profile acl STATEFUL_ACL
  permit 1 connection-state established related

dns-server
  host 10.10.10.1 sbc1.yourdomainname.com
  relay dns-client
  no shutdown

dns-client
  name-server 9.9.9.9
  name-server 8.8.8.8

profile dhcp-server DHCPS_LAN
  network 10.10.10.0/24
  lease 24 hours
  default-router 10.10.10.1
  domain-name-server 10.10.10.1
  include 10.10.10.2 10.10.10.100

profile tls DEFAULT
  authentication incoming
  authentication outgoing
  private-key pki:private-key/DEFAULT
  own-certificate 1 pki:certificate/DEFAULT
  diffie-hellman-parameters pki:diffie-hellman-parameters/DEFAULT-2048

profile tls PF_TLS_TEAMS
  no protocol tls-v1.0
  no protocol tls-v1.1
  compression
  authentication incoming
  authentication outgoing
  private-key pki:private-key/sbc1.yourdomainname.com.key
```

Set your preferred NTP server(s) as source. These can be either in your private or in the public network.

This ACL will be applied on the WAN interface of the context IP in incoming direction, in order permit incoming traffic only from the IP subnets from Microsoft. Additionally, you should add any relevant IP address / subnet like your company's own subnet or VPN (shown as xxx) from which you might need to access the unit from the internet.

This ACL will be applied on the WAN interface of the context IP in outgoing direction.

10.10.10.1 is the IP# of the LAN interface of the SBC in our setup. The example on the left is used if static translations as well as relay functionality (forwarding of DNS queries from LAN) are required. If not, just ignore and set it to shutdown.

Configure your preferred DNS servers, which can be either local or public.

DHCP profile, to be applied to the LAN network (see context IP further below), only if SBC's DHCP server functionality is required by the clients on the LAN, otherwise ignore it. If used, then def. GW, DNS server and DHCP range must be set accordingly, like in this example.

TLS profile for Teams Direct Routing. Force TLS v1.2 only by disabling v1.0 & v1.1. Assign the private key used for the certificate request and the imported signed X.509 certificate containing the SBC FQDN (.crt file). If an intermediary CA between the root certificate and the personal certificate is used, then assign also the intermediary CA.

```
  own-certificate 1 pki:certificate/sbc1.yourdomainname.com.crt
  own-certificate 2 pki:certificate/CA
  diffie-hellman-parameters pki:diffie-hellman-parameters/DEFAULT-4096
  require certificate-type server

profile tone-set DEFAULT

profile voip DEFAULT
  codec 1 g711alaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
  codec 2 g711ulaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
  codec 3 g729 rx-length 20 tx-length 20 silence-suppression
  media-processing forced
  rtp rtcp-multiplexing
  silence-suppression

profile voip PF_VOIP_MICROSOFT
  codec silk-16k negotiate
  codec silk-8k negotiate
  codec 1 g711alaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
  codec 2 g711ulaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
  srtp key-lifetime 31
  media-processing forced
  srtp transmission forced
  rtp rtcp-multiplexing
  silence-suppression

profile rip DEFAULT

profile sip DEFAULT

context ip ROUTER

  interface WAN
    ipaddress WAN AAA.BBB.CCC.DDD/EE
    use profile acl in 1 ACL_WAN_IN_DENY
    use profile acl in 2 STATEFUL_ACL
    use profile acl out 1 ACL_WAN_PROTOCOLS
    use profile acl out 2 STATEFUL_ACL
    use profile napt NAPT_WAN WAN

  interface LAN
    ipaddress LAN 10.10.10.1/24

  routing-table DEFAULT
    route 0.0.0.0/0 gateway AAA.BBB.CCC.FFF metric 0

  bgp
    shutdown

  rip
    shutdown

context ip ROUTER
  use profile dhcp-server DHCPS_LAN

nodems-client
  organization-key XXXXXXX
  resource any
  call-reporting forced
  no shutdown

profile ppp DEFAULT

cwmp-client
  shutdown

  stun
    shutdown
```

Default VoIP profile, which will be applied to any SIP interface if no specific profile is assigned. In our case the SIP-Trunk towards VoIP provider will use it.

Important: the VoIP parameter **media-processing forced** allows to **force the use of hardware DSP resources for all calls**, including also scenarios where the same codec can be negotiated on both legs of the call.
The highlighted settings fulfill the specific requirements of Microsoft for the full certification in terms of: 1) RTCP packets generation by SBC when these are not generated by SIP-Trunk, 2) Generation of Comfort Noise by the SBC when the call is muted by either PSTN or Teams, 3) RTCP multiplexing
If transcoding is not mandatory, remove the command-line **media-processing forced.**

Dedicated VoIP profile for MS Teams, which will be applied to the three SIP interfaces for Teams (1 per remote FQDN).

Important: the VoIP parameter **media-processing forced** allows to **force the use of hardware DSP resources for all calls**, including also scenarios where the same codec can be negotiated on both legs of the call.
The highlighted settings fulfill the specific requirements of Microsoft for the full certification in terms of: 1) RTCP packets generation by SBC when these are not generated by SIP-Trunk, 2) Generation of Comfort Noise by the SBC when the call is muted by either PSTN or Teams, 3) RTCP multiplexing
If transcoding is not mandatory, remove the command-line **media-processing forced.**

Set the static public IP address / subnet mask of the WAN interface of the SBC. The FQDN of the SBC must be resolved with this IP address in the public network. Apply previously defined ACLs in the corresponding directions.

Define the IP address / subnet mask of the LAN interface of the SBC (if required).
Define the default route and, if necessary, any static routes required by your network environment.

Set the Organization Key of your Patton Cloud environment, which you will register your SBC device to.
Call-reporting forced means CDR's collection will be used for this device (if the corresponding Cloud Service Plan is available).

```
context cs SWITCH

  mapping-table calling-e164 to calling-e164 MT_PEOPLEFONE_TO_TEAMS_CNPN
    map 00(.%) to \+\1
    map 0(.%) to \+41\1

  mapping-table called-e164 to called-e164 MT_PEOPLEFONE_TO_TEAMS_CDPN
    map (.%) to \+\1

  mapping-table calling-uri to calling-pi MT_TEAMS_TO_PEOPLEFONE_CNURI_CNPI
    map default to allowed
    map sip:anonymous@anonymous.invalid to restricted

  mapping-table calling-uri to calling-second-pi MT_TEAMS_TO_PEOPLEFONE_CNURI_CNPI2
    map default to allowed
    map sip:anonymous@anonymous.invalid to restricted

  mapping-table called-uri to called-uri MT_TEAMS_TO_PEOPLEFONE_CDURI
    map sip:\+(.%)@(.%) to sip:\1@\2


  routing-table called-e164 RT_FROM_PEOPLEFONE
    route 4131999990[1-4] dest-service HG_MS_FAILOVER CF_PEOPLEFONE_TO_TEAMS

  routing-table called-e164 RT_FROM_TEAMS
    route default dest-interface IF_SIP_PEOPLEFONE_TRUNK CF_TEAMS_TO_PEOPLEFONE

  complex-function CF_PEOPLEFONE_TO_TEAMS
    execute 1 MT_PEOPLEFONE_TO_TEAMS_CNPN
    execute 2 MT_PEOPLEFONE_TO_TEAMS_CDPN

  complex-function CF_TEAMS_TO_PEOPLEFONE
    execute 1 MT_TEAMS_TO_PEOPLEFONE_CNURI_CNPI
    execute 2 MT_TEAMS_TO_PEOPLEFONE_CNURI_CNPI2
    execute 3 MT_TEAMS_TO_PEOPLEFONE_CDURI

  interface sip IF_SIP_PEOPLEFONE_TRUNK
    bind context sip-gateway GW_PEOPLEFONE_TRUNK
    route call dest-table RT_FROM_PEOPLEFONE
    remote peoplefone.com
    local peoplefone.com
    hold-method direction-attribute inactive
    no call-transfer emit
    call-reroute emit
    history-info emit
    privacy
    uri-scheme sip
    session-timer 1800 method re-invite


  interface sip IF_SIP_TEAMS_1
    bind context sip-gateway GW_TEAMS
    route call dest-table RT_FROM_TEAMS
    remote sip.pstnhub.microsoft.com 5061
    local sbc1.yourdomainname.com 5067
    hold-method direction-attribute inactive
    no call-transfer accept
    privacy
    address-translation incoming-call calling-uri from-header
    use profile voip PF_VOIP_MICROSOFT
    penalty-box sip-option-trigger interval 60 timeout 60 force tls
    session-timer 1800 method re-invite

  interface sip IF_SIP_TEAMS_2
    bind context sip-gateway GW_TEAMS
    route call dest-table RT_FROM_TEAMS
    remote sip2.pstnhub.microsoft.com 5061
    local sbc1.yourdomainname.com 5067
    hold-method direction-attribute inactive
    no call-transfer accept
```

Mapping tables for (Inbound) SIP calls from VoIP provider Peoplefone CH towards Teams, which convert the phone numbers to E164 format.

The two particular mapping tables below concern the Outgoing calls. They are necessary because Teams always sends PAI and Privacy: id, if PAI forwarding is active, even if the outgoing call is not anonymous (restricted id.). With these two mappings, the SBC forces the Presentation Indicator to allowed for non-anonymous calls, otherwise sets it to restricted for anonymous calls.

This MT only removes the leading '+' in the called-uri from Teams.

RT from PSTN to Teams: use your DDI range here.
RT from Teams to PSTN;

Complex function calling the defined Mapping tables for the direction PSTN -> Teams.

Complex function calling the defined Mapping tables for the direction Teams -> PSTN.

SIP interface for PSTN (Peoplefone CH)
Remote: host part of TO Header in outgoing requests.
Local: host part of FROM Header in outgoing requests.
Preferred hold method: inactive.
History-Info header required for forwarded calls (PSTN1 -> Teams -> Call forward to PSTN2)
Privacy: enables Identity Restriction support according to RFC.
Session refresh method: re-Invite (default). Can also be set to Update if required (from SW version 3.20.2 on).

SIP interface for MS Teams / primary Datacenter.
Remote: fix setting to sip.pstnhub.microsoft.com 5061
Local: insert your SBC's FQDN + SIP listening port (if you set 5067 here, you must set the same port number in CsOnlinePSTNGateway -SipSignallingPort on Teams Management side.)
Hold method: inactive (as required by MS).
Apply previously defined VoIP profile for MS Teams.
60 means SBC sends SIP OPTIONS every 60 seconds.

SIP interface for MS Teams / secondary Datacenter.
Remote: fix setting to sip2.pstnhub.microsoft.com 5061

(rest of setting identical to the 1st one)

```
    privacy
    address-translation incoming-call calling-uri from-header
    use profile voip PF_VOIP_MICROSOFT
    penalty-box sip-option-trigger interval 60 timeout 60 force tls
    session-timer 1800 method re-invite

  interface sip IF_SIP_TEAMS_3
    bind context sip-gateway GW_TEAMS
    route call dest-table RT_FROM_TEAMS
    remote sip3.pstnhub.microsoft.com 5061
    local sbc1.yourdomainname.com 5067
    hold-method direction-attribute inactive
    no call-transfer accept
    privacy
    address-translation incoming-call calling-uri from-header
    use profile voip PF_VOIP_MICROSOFT
    penalty-box sip-option-trigger interval 60 timeout 60 force tls
    session-timer 1800 method re-invite
```

SIP interface for MS Teams / tertiary Datacenter.
Remote: fix setting to sip3.pstnhub.microsoft.com 5061

(rest of setting identical to the 1st one)

```
  service hunt-group HG_MS_FAILOVER
    timeout 3
    drop-cause normal-unspecified
    drop-cause no-circuit-channel-available
    drop-cause network-out-of-order
    drop-cause temporary-failure
    drop-cause switching-equipment-congestion
    drop-cause access-info-discarded
    drop-cause circuit-channel-not-available
    drop-cause resources-unavailable
    route call 1 dest-interface IF_SIP_TEAMS_1
    route call 2 dest-interface IF_SIP_TEAMS_2
    route call 3 dest-interface IF_SIP_TEAMS_3
```

Service Hunt-Group used for the failover mechanism, which covers both of these two scenarios:

- Primary / Secondary DC not reachable (no TCP connection)
- Primary / Secondary DC not responding (no response to SIP Request)

With the parameter Timeout you can adjust the duration (in seconds) after which the failover will take place in 2nd scenario.

```
context cs SWITCH
  no shutdown

authentication-service AS_SIP_PEOPLEFONE
  realm 1 AAA.BBB.CCC.DDD
  realm 2 peoplefone.com
  username USERNAME1 password XXXXXXX

location-service LS_PEOPLEFONE_TRUNK
  domain 1 peoplefone.com

  identity-group DEFAULT
    alias expression .[0-9]+
    user phone

    authentication outbound
      authenticate 1 authentication-service AS_SIP_PEOPLEFONE username USERNAME1

    registration outbound
      registrar sips.peoplefone.ch
      uri-scheme sip
      transport-protocol force udp
      lifetime 1800
      register auto

    call outbound
      force-destination registrar address
      transport-protocol force udp

  identity USERNAME1 inherits DEFAULT
```

Authentication user name and password for the SIP-Trunk of the VoIP Provider Peoplefone. Set the SBC's public IP# as realm 1 (one realm used for SIP-Trunk, another realm used for an optional SIP line).

```
location-service LS_TEAMS
  domain 1 microsoft.com
  domain 2 sip-du-a-eu.pstnhub.microsoft.com
  domain 3 sip-du-a-us.pstnhub.microsoft.com
  domain 4 sip-du-a-as.pstnhub.microsoft.com
  domain 5 sip-du-a-au.pstnhub.microsoft.com
  domain 6 pstnhub.microsoft.com
  domain 7 sip.pstnhub.microsoft.com
  domain 8 sip2.pstnhub.microsoft.com
  domain 9 sip3.pstnhub.microsoft.com
  domain 10 anonymous.invalid

  identity-group DEFAULT
```

Location Service configuration part for Teams: in this config. scenario it is used to:
1) respect the Request-URI recommendation to have user=phone parameter to simplify the call setup process on Teams side.
2) filter the host parts according to the ones effectively used by Microsoft (anonymous.invalid required for calls with restricted Id. From Teams)

```
  user phone

  authentication inbound
    authenticate none

  call outbound

  call inbound

sip
  no lock-dns-record

context sip-gateway GW_PEOPLEFONE_TRUNK
  bind location-service LS_PEOPLEFONE_TRUNK

  interface IF_GW_PEOPLEFONE_TRUNK
    transport-protocol udp+tcp 5060
    no transport-protocol tls
    bind ipaddress ROUTER WAN WAN

context sip-gateway GW_PEOPLEFONE_TRUNK
  no shutdown

context sip-gateway GW_TEAMS
  use profile tls PF_TLS_TEAMS
  bind location-service LS_TEAMS

  interface IF_GW_TEAMS
    no transport-protocol udp+tcp
    transport-protocol tls 5067
    bind ipaddress ROUTER WAN WAN
    spoofed contact-header manual sbc1.yourdomainname.com port 5067
    spoofed via-header manual sbc1.yourdomainname.com port 5067

context sip-gateway GW_TEAMS
  no shutdown

sip-survivability
  shutdown

port ethernet 0 0
  bind interface ROUTER WAN
  no shutdown

port ethernet 0 1
  bind interface ROUTER LAN
  no shutdown
```

Context SIP Gateway for Teams Direct Routing: bind it to the previously defined Location Service. Also apply the previously configured dedicated TLS profile for Teams.
Set transport protocol to TLS, and port number to the same one as you set in CsOnlinePSTNGateway -SipSignallingPort setting on Teams Management side (5067 in our example).
Spoofed Contact-Header: set manually to your SBC FQDN + port number

4.4.3Configuration sample for topology 3

This is the SN5501 SBC configuration file sample for the topology 3 described before, i.e. **Teams Direct Routing with an IPPBX**. The SIP-Trunk towards PSTN is realized through the IPPBX, meaning through LAN interface (no direct interface between SBC and VoIP provider). The example below more precisely refers to the tested setup with the telephony system STARFACE, based on Asterisk. For other IPPBX vendors, the SIP interface configuration might be slightly different, but the basics of the configuration remain identical.

Configuration parts highlighted in green: fix parts mandatory for Teams Direct Routing

Configuration parts highlighted in yellow: variable / project specific parts, that must be set to values that depend on the environment (IP addresses, domain names, SIP Gateway names containing IPPBX model name, routing/mapping table names with IPPBX model name …)

Not highlighted parts: recommended to leave as displayed but may be changed to other values depending on your needs.

Text boxes in case of this configuration template have been added only in the IPPBX specific parts, as all the other parts remain unchanged compared to topology 1.

Working principle: all inbound calls (from PSTN to IPPBX / Teams) and outbound calls (from IPPBX / Teams to PSTN) are routed through IPPBX and SBC.

Each IPPBX user who additionally has Teams enabled, must have an additional SIP device for Teams created in the user database. For each such user, an outgoing SIP registration from the SBC must be configured. This will allow the IPPBX to fork inbound calls also to the Teams user (beside the main SIP phone), so that both ring in parallel. The called user has the possibility to pick up the call on either IPPBX device or in Teams client. In the opposite way, i.e. in case of outbound calls, IPPBX will allow the call routing originating from Teams with the same user identity as if the call were setup from his main SIP device.

In both ways the correct user identity must be matched, and this is the work of our SBC through the specific mapping tables added for this use case.

```
#-----------------------------------------------------------------#
#                                                                 #
# Patton Electronics Company                                      #
# SN5501/8P v1.6 (SmartNode 5501 VoIP eSBC)                       #
# S/N: 00A0BAXXXXXX                                               #
# Release: 3.18.2-20122 2020/11/19                                #
# Generated configuration file                                    #
#                                                                 #
#-----------------------------------------------------------------#

cli version 4.00
superuser superuser password XXXXXXX
system hostname sbc1.yourdomainname.com
system description "SBC connected to MS Teams"
system location "Patton Inalp - Bern CH"
clock local default-offset +01:00
clock local dst-rule SUMMERTIME +1:00 from mar last sunday 02:00 2019 until oct last sunday
03:00 2036

profile aaa DEFAULT
  method 1 nodems continue-on-reject
  method 2 local
  method 3 none

console
  use profile aaa DEFAULT

telnet-server
  use profile aaa DEFAULT
  shutdown

ssh-server
  use profile aaa DEFAULT
  no shutdown

snmp-server
  shutdown

web-server
  no protocol http
  protocol https port 443
  use profile aaa DEFAULT
  no shutdown

ntp
  server 0.patton.pool.ntp.org
  server 1.patton.pool.ntp.org
  server 2.patton.pool.ntp.org
  server 3.patton.pool.ntp.org
  no shutdown

profile napt NAPT_WAN
```

```
profile acl ACL_WAN_IN_DENY
  permit 1 protocol tcp src-ip 52.112.0.0/14 dest-port 5061
  permit 2 protocol tcp src-ip 52.120.0.0/14 dest-port 5061
  permit 3 src-ip XXX.XXX.XXX.XXX/XX

profile acl ACL_WAN_PROTOCOLS
  permit 1 protocol udp dest-port 53,123,5060,5061
  permit 2 protocol tcp dest-port 53,443,5060,5061
  permit 3 protocol icmp

profile acl STATEFUL_ACL
  permit 1 connection-state established related

dns-server
  host 10.10.10.1 sbc1.yourdomainname.com
  relay dns-client
  no shutdown

dns-client
  name-server 9.9.9.9
  name-server 8.8.8.8

profile dhcp-server DHCPS_LAN
  network 10.10.10.0/24
  lease 24 hours
  default-router 10.10.10.1
  domain-name-server 10.10.10.1
  include 10.10.10.2 10.10.10.100

profile tls DEFAULT
  authentication incoming
  authentication outgoing
  private-key pki:private-key/DEFAULT
  own-certificate 1 pki:certificate/DEFAULT
  diffie-hellman-parameters pki:diffie-hellman-parameters/DEFAULT-2048

profile tls PF_TLS_TEAMS
  no protocol tls-v1.0
  no protocol tls-v1.1
  compression
  authentication incoming
  authentication outgoing
  private-key pki:private-key/sbc1.yourdomainname.com.key
  own-certificate 1 pki:certificate/sbc1.yourdomainname.com.crt
  own-certificate 2 pki:certificate/CA
  diffie-hellman-parameters pki:diffie-hellman-parameters/DEFAULT-4096
  require certificate-type server

profile tone-set DEFAULT

profile voip DEFAULT
  codec 1 g711alaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
  codec 2 g711ulaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
  codec 3 g729 rx-length 20 tx-length 20 silence-suppression
  media-processing forced
  rtp rtcp-multiplexing
  silence-suppression
```

VoIP profile that will be assigned to the SIP interface for PSTN. If SBC transcoding is not mandatory, remove “media-processing forced” from all VoIP profiles.

```
profile voip PF_VOIP_MICROSOFT
  codec silk-16k negotiate
  codec silk-8k negotiate
  codec 1 g711alaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
  codec 2 g711ulaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
  srtp key-lifetime 31
  media-processing forced
  srtp transmission forced
  rtp rtcp-multiplexing
  silence-suppression
```

VoIP profile that will be assigned to the SIP interface for Teams. If SBC transcoding is not mandatory, remove “media-processing forced” from all VoIP profiles.

```
profile voip PF_VOIP_STARFACE
  codec 1 g711alaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
  media-processing forced
```

```
  rtp rtcp-multiplexing

profile rip DEFAULT

profile sip DEFAULT

context ip ROUTER

  interface WAN
    ipaddress WAN AAA.BBB.CCC.DDD/EE
    use profile acl in 1 ACL_WAN_IN_DENY
    use profile acl in 2 STATEFUL_ACL
    use profile acl out 1 ACL_WAN_PROTOCOLS
    use profile acl out 2 STATEFUL_ACL
    use profile napt NAPT_WAN WAN

  interface LAN
    ipaddress LAN 10.10.10.1/24

  routing-table DEFAULT
    route 0.0.0.0/0 gateway AAA.BBB.CCC.FFF metric 0

  bgp
    shutdown

  rip
    shutdown

context ip ROUTER
  use profile dhcp-server DHCPS_LAN

nodems-client
  organization-key XXXXXXX
  resource any
  call-reporting forced
  no shutdown

profile ppp DEFAULT

cwmp-client
  shutdown

  stun
    shutdown

context cs SWITCH

  mapping-table called-uri to called-e164 MT_STARFACE_TO_TEAMS_CDURI_TO_CDPN
    map sip:teams_user_01@.+ to +41319999901
    map sip:teams_user_02@.+ to +41319999902
    map sip:teams_user_03@.+ to +41319999903
    map sip:teams_user_04@.+ to +41319999904

  mapping-table calling-uri to calling-pi MT_TEAMS_TO_STARFACE_CNURI_CNPI
    map default to allowed
    map sip:anonymous@anonymous.invalid to restricted

  mapping-table calling-uri to calling-second-pi MT_TEAMS_TO_STARFACE_CNURI_CNPI2
    map default to allowed
    map sip:anonymous@anonymous.invalid to restricted

  mapping-table calling-e164 to calling-uri MT_TEAMS_TO_STARFACE_CNPN_TO_CNURI
    map \+41319999901 to sip:teams_user_01@10.10.10.200
    map \+41319999902 to sip:teams_user_02@10.10.10.200
    map \+41319999903 to sip:teams_user_03@10.10.10.200
    map \+41319999904 to sip:teams_user_04@10.10.10.200

  mapping-table called-e164 to called-e164 MT_TEAMS_TO_STARFACE_INTERNAL_CDPN
    map (00)?41(...?)$ to \2

  routing-table called-e164 RT_FROM_STARFACE
    route default dest-service HG_MS_FAILOVER CF_STARFACE_TO_TEAMS

  routing-table called-e164 RT_FROM_TEAMS
    route default dest-interface IF_SIP_STARFACE CF_TEAMS_TO_STARFACE
```

VoIP profile that will be assigned to the SIP interface for IPPBX. If SBC transcoding is not mandatory, remove “media-processing forced” from all VoIP profiles.

```
complex-function CF_STARFACE_TO_TEAMS
  execute 1 MT_STARFACE_TO_TEAMS_CDURI_TO_CDPN

complex-function CF_TEAMS_TO_STARFACE
  execute 1 MT_TEAMS_TO_STARFACE_CNURI_CNPI
  execute 2 MT_TEAMS_TO_STARFACE_CNURI_CNPI2
  execute 3 MT_TEAMS_TO_STARFACE_CNPN_TO_CNURI
  execute 4 MT_TEAMS_TO_STARFACE_INTERNAL_CDPN
```

Complex function calling all the MT's in for the routing direction IPPBX -> Teams

Complex function calling all the MT's in for the routing direction Teams -> IPPBX

```
interface sip IF_SIP_STARFACE
  bind context sip-gateway GW_SIP_LAN
  route call dest-table RT_FROM_STARFACE
  remote starface.yourdomainname.com
  hold-method direction-attribute sendonly
  early-disconnect
  no call-transfer accept
  no call-transfer emit
  history-info emit
  address-complete-indication accept set
  address-translation incoming-call calling-e164 from-header
  address-translation incoming-call calling-uri from-header
  address-translation incoming-call calling-name from-header
  use profile voip PF_VOIP_STARFACE
  session-timer 1800 method re-invite
  trust remote

interface sip IF_SIP_TEAMS_1
  bind context sip-gateway GW_TEAMS
  route call dest-table RT_FROM_TEAMS
  remote sip.pstnhub.microsoft.com 5061
  local sbc1.yourdomainname.com 5067
  hold-method direction-attribute inactive
  no call-transfer accept
  privacy
  address-translation incoming-call calling-uri from-header
  use profile voip PF_VOIP_MICROSOFT
  penalty-box sip-option-trigger interval 60 timeout 60 force tls
  session-timer 1800 method re-invite

interface sip IF_SIP_TEAMS_2
  bind context sip-gateway GW_TEAMS
  route call dest-table RT_FROM_TEAMS
  remote sip2.pstnhub.microsoft.com 5061
  local sbc1.yourdomainname.com 5067
  hold-method direction-attribute inactive
  no call-transfer accept
  privacy
  address-translation incoming-call calling-uri from-header
  use profile voip PF_VOIP_MICROSOFT
  penalty-box sip-option-trigger interval 60 timeout 60 force tls
  session-timer 1800 method re-invite

interface sip IF_SIP_TEAMS_3
  bind context sip-gateway GW_TEAMS
  route call dest-table RT_FROM_TEAMS
  remote sip3.pstnhub.microsoft.com 5061
  local sbc1.yourdomainname.com 5067
  hold-method direction-attribute inactive
  no call-transfer accept
  privacy
  address-translation incoming-call calling-uri from-header
  use profile voip PF_VOIP_MICROSOFT
  penalty-box sip-option-trigger interval 60 timeout 60 force tls
  session-timer 1800 method re-invite

service hunt-group HG_MS_FAILOVER
  timeout 3
  drop-cause normal-unspecified
  drop-cause no-circuit-channel-available
  drop-cause network-out-of-order
  drop-cause temporary-failure
  drop-cause switching-equipment-congestion
  drop-cause access-info-discarded
  drop-cause circuit-channel-not-available
  drop-cause resources-unavailable
  route call 1 dest-interface IF_SIP_TEAMS_1
```

SIP interface for STARFACE IPPBX.
As remote, use either the domain name or the IP address of your IPPBX.

```
    route call 2 dest-interface IF_SIP_TEAMS_2
    route call 3 dest-interface IF_SIP_TEAMS_3

context cs SWITCH
  no shutdown

authentication-service AS_STARFACE SIP ACCOUNTS
  username teams_user_01 password teamsuserpassword01
  username teams_user_02 password teamsuserpassword02
  username teams_user_03 password teamsuserpassword03
  username teams_user_04 password teamsuserpassword04

location-service LS_STARFACE

  domain 1 starface.yourdomainname.com

  identity-group DEFAULT

    authentication outbound
      authenticate 1 authentication-service AS_STARFACE_SIP_ACCOUNTS

    authentication inbound
      authenticate none

    registration outbound
      registrar starface.yourdomainname.com
      lifetime 180
      register auto

    call outbound

    call inbound

    identity teams_user_01 inherits DEFAULT
    identity teams_user_02 inherits DEFAULT
    identity teams_user_03 inherits DEFAULT
    identity teams_user_04 inherits DEFAULT

location-service LS_TEAMS
   domain 1 microsoft.com
   domain 2 sip-du-a-eu.pstnhub.microsoft.com
   domain 3 sip-du-a-us.pstnhub.microsoft.com
   domain 4 sip-du-a-as.pstnhub.microsoft.com
   domain 5 sip-du-a-au.pstnhub.microsoft.com
   domain 6 pstnhub.microsoft.com
   domain 7 sip.pstnhub.microsoft.com
   domain 8 sip2.pstnhub.microsoft.com
   domain 9 sip3.pstnhub.microsoft.com
   domain 10 anonymous.invalid

   identity-group DEFAULT
     user phone

     authentication inbound
       authenticate none

     call outbound

     call inbound

sip
  no lock-dns-record

context sip-gateway GW_SIP_LAN
  bind location-service LS_STARFACE

  interface IF_GW_SIP_LAN
    transport-protocol udp+tcp 5060
    no transport-protocol tls
    bind ipaddress ROUTER LAN LAN

context sip-gateway GW_SIP_LAN
  no shutdown

context sip-gateway GW_TEAMS
  use profile tls PF_TLS_TEAMS
  bind location-service LS_TEAMS
```

Each IPPBX user that has Teams user rights must be created in this Authentication & Location service database, namely with exactly the same SIP credentials as on the IPPBX. The SBC will perform an outgoing SIP Registration towards IPPBX Registrar for each user.

```
  interface IF_GW_TEAMS
    no transport-protocol udp+tcp
    transport-protocol tls 5067
    bind ipaddress ROUTER WAN WAN
    spoofed contact-header manual sbc1.yourdomainname.com port 5067
    spoofed via-header manual sbc1.yourdomainname.com port 5067

context sip-gateway GW_TEAMS
  no shutdown

sip-survivability
  shutdown

port ethernet 0 0
  bind interface ROUTER WAN
  no shutdown

port ethernet 0 1
  bind interface ROUTER LAN
  no shutdown
```

5 Contacting Patton Support

Patton Electronics offers a wide array of technical services.

https://www.patton.com/support/support.asp

Region	Western Europe	North America	Central & Eastern Europe
Location	Bern, CH	Maryland, USA	Budapest, HU
Time Zone	CET / CEST UTC +1h (+2h)	ET / EST UTC -4h (-5h)	CET / CEST UTC +1h (+2h)
Business hours	Monday – Friday 09:00 to 12:00 13:30 to 17:30	Monday – Friday 8:00 am to 5:00 pm	Monday – Friday 08:30 to 17:00
E-Mail	support@patton.com	support@patton.com	support@patton.com
Phone	+41 31 985 25 55	+1 301 975 1007	+36 1 439 4835
Fax	+41 31 985 25 26	+1 301 869 9293	