

Using Teams with the Sentinel PBX only Scenario

Sentinel series

DGW 49.2.2941

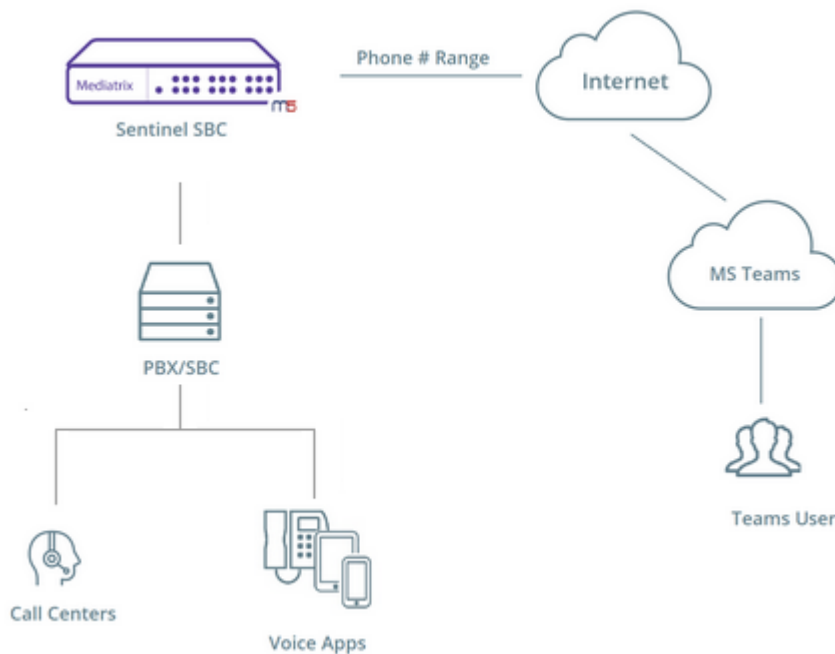
2023-08-09

Table of Contents

Microsoft Teams Direct Routing and Sentinel Interoperability PBX Scenario	3
Requirements for MS Teams	4
Connecting to MS Teams with PowerShell	5
Configuring MS Teams Voice Routing	5
Requirements for the Sentinel	7
Sentinel Set-Up for Teams	10
Importing Rulesets	10
Configuring the Local Firewall	11
Configuring the Signaling Interfaces	12
Configuring the Media Interfaces	13
Configuring the MS_Teams_Direct_Routing_ca Call Agent	14
Configuring the lan_ip_pbx_ca Call Agent	15
Associating Routing Ruleset to the Configuration	16
MS_Teams_to_pbx Routing Ruleset	17

Microsoft Teams Direct Routing and Sentinel Interoperability PBX Scenario

This configuration notes explains the required configuration to use Microsoft Teams with the Sentinel and an IP PBX.



The Sentinel SBC from Media5 is the Session Border Controller used in the Enterprise model of Microsoft. It terminates MS Direct Routing trunk and provides interconnections to various types of telephony endpoints, not covered on this document:

- External 3rd party SIP trunk
- PRI or FXS/FXO telephony interfaces to legacy PBX
- Analog telephone adaptors (ATA)

For more information on the Microsoft Direct Route planning, visit: <https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan>.

Requirements for MS Teams

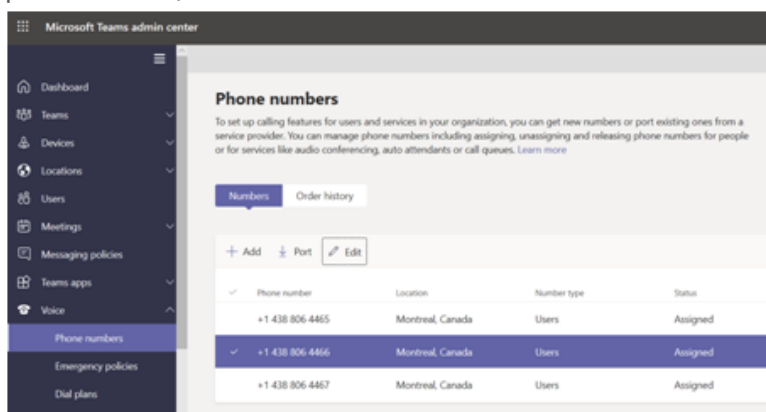
- Refer to the following link for MS Teams direct routing requirements: <https://docs.microsoft.com/en-us/microsoftteams/onboarding-checklist-enable-office-365>
- A publicly resolvable FQDN for the Sentinel. The FQDN must be in one of the domains defined under your Microsoft Teams account. For example the SBC FQDN is set to sbcteams.mediatrix.com, which is under the mediatrix.com domain.

Media5

Domains

+ Add domain Buy domain Refresh	
Domain name	Status
mediatrix.com (Default)	Healthy
mediatrixsbc.onmicrosoft.com	Healthy

- At least one Microsoft Teams user must be created under the same domain. In our example, we have created one such account: media5user@mediatrix.com
- DID Phone Numbers to dial in, you can get DID phone numbers under Microsoft Teams admin Center/Users/Phone Numbers and assign it to a specific user (or auto-attendant, which is a pseudo-user).



Connecting to MS Teams with PowerShell

Before you start

Microsoft Visual C++ 2017 x 64 Minimum Runtime - 14.10.25008 package must be installed.

Steps

- 1) Download and install Power Shell: <https://docs.microsoft.com/en-us/SkypeForBusiness/set-up-your-computer-for-windows-powershell/set-up-your-computer-for-windows-powershell>
- 2) Open PowerShell from your PC. Run it as Administrator.
- 3) Install Microsoft Teams module if needed: <https://docs.microsoft.com/en-us/MicrosoftTeams/teams-powershell-install#install-the-teams-powershell-module>
- 4) Type Set-executionPolicy -ExecutionPolicy RemoteSigned
- 5) Click **Yes** to all.
- 6) Enter Import-Module MicrosoftTeams
- 7) Enter Connect-MicrosoftTeams
- 8) Enter your tenant admin user name and password.

Next Step

[Configuring MS Teams Voice Routing \(p.5\)](#)

Configuring MS Teams Voice Routing

Information

Steps

- 1) In the MS Teams PowerShell, enter the command to create the Direct Routing SIP trunk.

Note: For example New-CsOnlinePSTNGateway -Fqdn sbcteams.mediatatrix.com -SipSignalingPort 5061 -MaxConcurrentSessions 5 -Enabled \$true
- 2) Enter the command to create the actual voice route that will be used to route calls to the SBC.

For example

```
Set-CsOnlinePstnUsage -Identity Global -Usage  
@{Add="Montreal514Sherbrooke819"}
```

and

```
New-CsOnlineVoiceRoute -Identity "Montreal Sherbrooke" -  
NumberPattern "^\\+1(514|819)(\\d{7})$"
```

```
-OnlinePstnGatewayList sbcteams.mediatrix.com -Priority 1 -  
OnlinePstnUsages "Montreal514Sherbrooke819"
```

and

```
New-CsOnlineVoiceRoutingPolicy "Montreal Sherbrooke" -  
OnlinePstnUsages "Montreal514Sherbrooke819"
```

- 3) Enter the command to assign the routing policy to the users.

Note: For example `Grant-CsOnlineVoiceRoutingPolicy -Identity "user1@mediatrix.com" -PolicyName "Montreal Sherbrooke"`

- 4) In case you need to assign an OnPremise number to specific user, enter the command:

Note: For example `Set-CsUser -Identity "user1@mediatrix.com" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true -OnPremLineURI tel:42565`

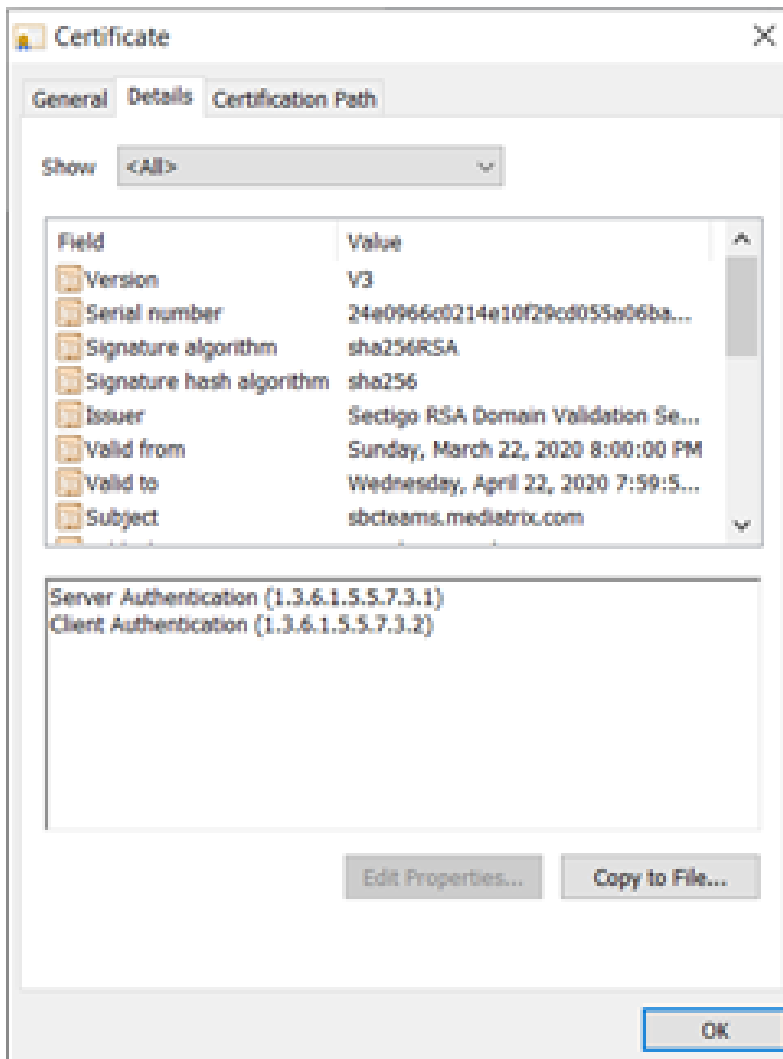
Next Step

[Importing Rulesets](#) (p.10)

Requirements for the Sentinel

- DGW software version: MediatrixSentinel_Dgw_48.0.2430 or newer.
- Rulesets created to use Teams with the Sentinel. Contact your sales representative.

- A server certificate with the SBC FQDN in the Common Name or Subject Alternative Name signed by one of the approved public CA by Microsoft. In our test, the SBC host certificate was signed by Comodo (one-month Free Trial):
 - Key length 2048 bits
 - Signature Hash algorithm: SHA 256
 - Extended Usage: ClientAuthentication and ServerAuthentication
 - Common Name: sbcteams.mediatrrix.com
 - SAN may contain wild card FQDN, most root CA will charge extra for that; the Comodo free trial does not allow that so it was skipped



- Generate the necessary CSR (Certificate Signing Request), and later combine the private key and the CA signed certificate to form a host certificate to upload to the Sentinel: Refer to <https://documentation.media5corp.com/display/DGWLATEST/Creating+a+Media5+Device+Host+Certificate+with+OpenSSL>

- Install Baltimore Cybertrust Root CA certificate on the SBC (<https://www.digicert.com/digicert-root-certificates.htm>); this is to validate against MS Teams servers (sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com, sip3.pstnhub.microsoft.com)
- Associate the host certificate to the SBC service. Make sure only 1 certificate is associated to it. Refer to <https://documentation.media5corp.com/display/DGWLATEST/Using+Trusted+CA+and+Host+Certificates> for more details.
- To speed up incoming calls from Teams, as calls from Teams Direct Routing server may come from another IP (not the same as the ones resolved by DNS), set up the following static DNS entries

```
Hoc.StaticHosts.DeleteAllRows
Hoc.InsertStaticHost Name="sip.pstnhub.microsoft.com"
IpAddresses="52.114.132.46,52.114.148.0,52.114.132.46,52.114.75.24,
52.114.76.76,52.114.7.24,52.114.14.70"

#the sequence of IP addresses may vary from region to region, ping MS
Teams FQDN
to find out what it is resolved into for your region
```

Note: There are also different FQDNs for US government and Department of Defense, please follow the MS Teams Direct Routing planning document. You can find the IP addresses for these domains there.

Sentinel Set-Up for Teams

The following is the Network topology tested in this setup.

- A FreePBX (peered to lan_ip_pbx_ca call agent) is used as the enterprise IP PBX. It has a SIP trunk pointing to the Sentinel SBC, signaling is plain UDP and media is un-encrypted RTP
- The Microsoft Direct Routing trunk is peered to the MS_Teams_Direct_Routing_ca call agent. The signaling with MS Teams is over TLS and media is encrypted with sRTP.
- The topology between FreePBX and MS Teams is as follows:
Polycom phone ⇄ FreePBX ⇄ sip trunk ⇄ Sentinel SBC ⇄ direct routing ⇄ MS Teams Cloud ⇄ Teams clients
- The Sentinel SBC is deployed behind a NAT firewall and only the Uplink interface is used. TCP port 5061, as well as UDP 21000-21010, are port forwarded to the SBC by the NAT firewall.

Importing Rulesets

Before you start

Rulesets must first be imported. Contact your sales representative to obtain the required rulesets to use Teams with the Sentinel.

Information

This procedure is valid for Call Agent and Routing Rulesets.

Steps

- 1) Go to **Management/File**.

Note: Step 2 is only required when importing the first Ruleset and if you are not using a secure connection to access the Management Interface (http://).

- 2) Click **Activate unsecure file importation from the Web browser**.
- 3) From the **Path** field, select sbc/rulesets/.
- 4) Click **Browse**, and navigate to the following Rulesets to import:
 - a) force_media_plain_rtp_handle_replaces.crs
 - b) MS_Teams_interop.crs
 - c) MS_Teams_PBX_routes.rrs

Note: Ruleset file extension must be *.crs for Call Agent Rulesets or *.rrs for Routing Rulesets.

- 5) Click **Import**.

Result

The imported Rulesets will appear in the **Internal files** table, with the selected path in front of the name. The Ruleset will be available in the tables of the **SBC/Rulesets** page.

Path	File
sbc/rulesets/	C:\Rulesets\your_ruleset

Browse ... Import

Next Step

[Configuring the Local Firewall \(p.11\)](#)

Configuring the Local Firewall

Information

Use this procedure if you cannot apply the specific firewall rules at the external NAT firewall outlined in the Microsoft Direct Routing Planning guide: <https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan>

More information about configuring local firewall rules on DGW is available on: <https://documentation.media5corp.com/display/DGWLATEST/Configuring+Local+Firewalls>

Steps

- 1) Go to **Network/Local Firewall**.
- 2) In the **Local Firewall Rules** table, complete the fields for each rule managing the TCP packets as follows:
 - a) **Activation: Enable**
 - b) **Source Address:** IP address of the TCP incoming packet.
 - c) **Destination Address: Uplink**
 - d) **Protocol: TCP**
 - e) **Destination Port:** 5061
 - f) **Action: Accept**
- 3) Complete the fields for each rule managing the UDP packets as follows:
 - a) **Activation: Enable**
 - b) **Source Address:** IP address of the UDP incoming packet.
 - c) **Destination Address: Uplink**
 - d) **Source Port:** Source port of the incoming UDP packet.
 - e) **Protocol: UDP**
 - f) **Destination Port=**30000-30999
 - g) **Action: Accept**
- 4) Click **Save & Apply**.

Result

For example

1	Enable	52.114.75.24		Uplink	5061	TCP		Accept	10	60				
2	Enable	52.114.148.0		Uplink	5061	TCP		Accept	10	60				
3	Enable	52.114.132.46		Uplink	5061	TCP		Accept	10	60				
4	Enable	52.114.7.24		Uplink	5061	TCP		Accept	10	60				
5	Enable	52.114.76.76		Uplink	5061	TCP		Accept	10	60				
6	Enable	52.114.14.70		Uplink	5061	TCP		Accept	10	60				
7	Enable	52.114.16.74		Uplink	5061	TCP		Accept	10	60				
8	Enable	52.114.20.29		Uplink	5061	TCP		Accept	10	60				
9	Enable	52.114.36.156		Uplink	5061	TCP		Accept	10	60				
10	Enable	52.114.32.169		Uplink	5061	TCP		Accept	10	60				
11	Enable			Uplink	5061	TCP		Drop	10	60				
12	Enable	52.112.0.0/14	49152-53247	Uplink	30000-30999	UDP		Accept	10	60				
13	Enable	52.112.0.0/14	3478-3481	Uplink	30000-30999	UDP		Accept	10	60				
14	Enable	52.120.0.0/14	49152-53247	Uplink	30000-30999	UDP		Accept	10	60				
15	Enable	52.120.0.0/14	3478-3481	Uplink	30000-30999	UDP		Accept	10	60				

Next Step

Configuring the Signaling Interfaces (p.12)

Configuring the Signaling Interfaces

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Signaling Interface Configuration** cable, configure the pbx_s as follows:
 - a) **Name:** pbx_s
 - b) **Network:** Uplink
 - c) **Port:** 5062
 - d) **Secure Port :** 5063
 - e) **Allowed Transport:** All
 - f) **TLS Mode:** Client
 - g) **Public Address:** leave empty

Note: This is the signaling interface used by the LAN IP PBX (no NAT)

- 3) Click **+** and complete the fields as follows.
- Name:** teams_s
 - Network:** Uplink
 - Port:** 5060
 - Secure Port :** 5061
 - Allowed Transport:** TlsOnly
 - TLS Mode:** Both
 - Public Address:** FQDN assigned to the SBC

Note: This is the signaling interface used by MS Teams (interface set to TLS only), the public address field must contain the FQDN assigned to the SBC (this is mandatory for MS Teams to require the FQDN in the SIP Contact host part, otherwise it will reply with a SIP 403 Forbidden)

Result

Signaling Interface Configuration							
Name	Network	Port	Secure Port	Allowed Transports	Tls Mode	Public Address	
loop_s	Loop	0	0	All	Client		-
lan1_s	Lan1	0	0	All	Client		-
pbx_s	Uplink	5062	5063	All	Client		-
teams_s	Uplink	0	5061	TlsOnly	Both	SBC FQDN	-
							+

Next Step

[Configuring the Media Interfaces \(p.13\)](#)

Configuring the Media Interfaces

Information

Steps

- Go to **SBC/Configuration**.
- in the **Media Interface Configuration** table, configure the pbx_m Media interface as follows:
 - Name:** pbx_m
 - Network:** Uplink
 - Port Range:** 21000-21200
 - Public Address:** leave empty

Note: This is the media interface used by the LAN IP PBX (no NAT)

- 3) Click **+** and configure the fields as follows:
 - a) **Name:** teams_m
 - b) **Network:** Uplink
 - c) **Port Range:** 30000-30999
 - d) **Public Address:** external Public IP address of the SBC

Note: This is the media interface used by MS Teams (with near end NAT enabled, public IP address assigned)

Result

Media Interface Configuration					
Name	Network	Port Range	Public Address		
loop_m	Loop	20000-20999		-	
lan1_m	Lan1	20000-20999		-	
pbx_m	Uplink	21000-21200		-	
teams_m	Uplink	30000-30999	SBC public address	-	
				+	

Next Step

Configuring the MS_Teams_Direct_Routing_ca Call Agent

Configuring the MS_Teams_Direct_Routing_ca Call Agent

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Call Agent Configuration** table, click **+**.
- 3) In the **Configure Call Agent** table, complete the fields as follows:
 - a) **Name:** MS_Teams_Direct_Routing_ca
 - b) **Enable:** checked
 - c) **Signaling Interface:** teams_s
 - d) **Media Interface:** teams_m
 - e) **Peer Host:** sip.pstnhub.microsoft.com:5061
 - f) **Force Transport:** Tls
 - g) **Keep-Alive Interval:** 30
 - h) **Blacklisting Duration:** 60
 - i) **Blacklisting Delay:** 0
 - j) **Custom Header:** X-MS-SBC: Mediatrix/%productseries%/%version%
- 4) In the **Call Agent Rulesets** table, from the **Name** select MS_Teams_interop.
- 5) In the **Parameters** field, enter the CC=Country Code and the DIGITS=Number of digits of CC + 1, eg.CC=1 DIGITS=2, or CC=34 DIGITS=3.
- 6) Click **Save**.

Result

Configure Call Agent		Value
Call Agent Parameters		
Name	MS_Teams_Direct_Routing_ca	
Enable	☒	
Gateway		
Signaling Interface	teams_s	
Media Interface	teams_m	
Peer Host	sip.pstnhub.microsoft.com:5061	
Peer Network		
Force Transport	Tls	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	30	
Blacklisting Duration	60	
Blacklisting Delay	0	
Blacklisting Error Codes		
Custom Header	X-MS-SBC: Mediatix/%productseries%/%version%	

Call Agent Rulesets		
Priority	Name	Parameters
3	MS_Teams_interop	CC=1 DIGITS=2

Configuring the lan_ip_pbx_ca Call Agent

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Call Agent Configuration** table, click  located on the same line as lan_ip_pbx_ca
- 3) In the **Configure Call Agent** table, complete the fields as follows:
 - a) **Name:** lan_ip_pbx_ca
 - b) **Enable:** checked
 - c) **Signaling Interface:** pbx_s
 - d) **Media Interface:** pbx_m
 - e) **Peer Host:** IP address of the local IP PBX
 - f) **Force Transport:** none
 - g) **Keep-Alive Interval:** 30
 - h) **Blacklisting Duration:** 0
 - i) **Blacklisting Delay:** 0
- 4) In the **Call Agent Rulesets** table, from the **Name** select force_media_plain_rtp_handle_replaces
- 5) Click **Save**.

Result

Configure Call Agent		Value
Call Agent Parameters		
Name	lan_ip_pbx_ca	
Enable	☒	
Gateway		
Signaling Interface	pbx_s	
Media Interface	pbx_m	
Peer Host	IP address of local IP PBX	
Peer Network		
Force Transport	None	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	30	
Blacklisting Duration	0	
Blacklisting Delay	0	
Blacklisting Error Codes		
Custom Header		

Call Agent Rulesets		
Priority	Name	Parameters
1	force_media_plain_rtp_handle_replaces	
+		

Next Step

Associating Routing Ruleset to the Configuration (p.16)

Associating Routing Ruleset to the Configuration

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Routing Rulesets** table, click **+**.
- 3) From the **Name** selection list, choose MS_Teams_PBX_routes
- 4) Click **Apply**.

Result

Routing Rulesets		
Priority	Name	Parameters
1	MS_Teams_PBX_routes	
+		

MS_Teams_to_pbx Routing Ruleset

- If the MS Teams client dials any number, the call is routed to lan_ip_pbx_ca, i.e. FreePBX.
- If the call is initiated from the FreePBX, the call is routed to MS Teams, transport is forced to TLS.

MS_Teams_PBX_routes Routes between MS Teams and PBX		
Conditions	Actions	Active
Source Call Agent == "MS_Teams_Direct_Routing_ca"	Call agent: lan_ip_pbx_ca Next hop: [] Route via: Next hop Update R-URI host: 1 Update To-URI host: 1	✓
Source Call Agent == "lan_ip_pbx_ca"	Call agent: MS_Teams_Direct_Routing_ca Force transport: 1 Next hop: [] Route via: Next hop Transport protocol: TLS Update R-URI host: 1	✓



media5corp.com