Integrating with Microsoft Teams

Microsoft Teams Direct Routing integration connects Microsoft Teams users to MiRTA PBX through OpenSIPS and an Asterisk PJSIP TLS transport. Treat this integration as an advanced deployment task: test it on one tenant and one Teams user before applying it broadly.

Component	Role
Microsoft Teams	Hosts the Teams user, Direct Routing domain, SBC, voice route, PSTN usage record, and voice routing policy.
OpenSIPS	Listens for the Teams-side SIP/TLS connection and proxies it toward the Asterisk PJSIP listener.
Asterisk PJSIP	Terminates the PBX-side Teams trunk on a dedicated TLS transport, endpoint, AOR, and identify section.
MiRTA PBX	Stores the Teams integration settings, tenant Teams address, Microsoft Graph credentials, and custom extension authentication.

Prerequisites

- Use a public DNS name for the Teams SBC. The certificate must include every Teams-facing domain used by the integration.
- Prepare public reachability for the Teams/OpenSIPS side and the dedicated Asterisk PJSIP TLS listener.
- Use a Microsoft tenant with the required Teams Phone and Microsoft 365 licensing for Direct Routing.
- Plan a dedicated Teams test user and a MiRTA PBX custom extension for the first validation.
- Keep a rollback path for OpenSIPS, Asterisk PJSIP, and MiRTA PBX tenant settings before changing production routing.

Microsoft Teams Configuration

Configure Microsoft Teams for Direct Routing before activating the PBX side. Microsoft admin menu names may change, but the required objects are the domain, SBC, PSTN usage record, voice route, routing policy, and user phone assignment.

1. In the Microsoft 365 admin center, open **Settings > Domains** and add the SBC domain, for example `sbc.example.com`.
2. Verify the domain. DNS TXT verification is commonly used: copy the verification value from Microsoft and publish it in public DNS.
3. If this domain is used only for voice, leave Exchange-related services disabled during domain setup.
4. Create or update the Teams user that will be tested with Direct Routing.
5. Assign the required licenses, such as Teams Phone plus the appropriate Microsoft 365 plan.
6. In the Microsoft Teams admin center, open **Voice > Direct Routing**.
7. Create a PSTN usage record, for example `sbc`.
8. Add the SBC. Enable it and enable SIP OPTIONS so Teams can monitor SBC availability.
9. Create a voice route. Use a dialed-number pattern that matches the numbers you want to send to MiRTA PBX, for example `^(\+[0-9]{7,15})$` for E.164 numbers.
10. Attach the SBC and the PSTN usage record to the voice route.
11. Create a voice routing policy and add the PSTN usage record.
12. Assign the voice routing policy to the Teams user.
13. Assign a Direct Routing phone number to the user.

The SBC may show as inactive until OpenSIPS, certificates, and the Asterisk PJSIP transport are configured and reachable.

OpenSIPS Configuration

Install OpenSIPS on the node that will face Microsoft Teams. In the reference configuration, OpenSIPS listens on port 5067 and proxies traffic to the Asterisk PJSIP TLS listener on port 5091.

```
dnf config-manager --set-enabled crb
dnf -y install epel-release epel-next-release
dnf -y install https://yum.opensips.org/3.4/releases/st/9/x86_64/opensips-yum-releases-3.4-6.el9.noarch.rpm
yum -y install opensips opensips-* opensips-cli socat
systemctl enable opensips
```

Copy the prepared OpenSIPS configuration from the MiRTA PBX protected files to the OpenSIPS configuration directory:

```
cp /var/www/html/pbx/protected/opensips.cfg /etc/opensips/opensips.cfg
```

Adjust the placeholders in the OpenSIPS configuration before starting the service.

Placeholder	Meaning
`<IP-SERVER>`	Private or local IP address of the OpenSIPS virtual machine or node.
`<NAT-IP-SERVER>`	Public NAT address when NAT is used; otherwise use the same value as `<IP-SERVER>`.
`<IP-ASTERISK>`	IP address of the Asterisk server that receives proxied Teams traffic.
`<DOMAIN-ASTERISK>`	Fully qualified domain name used for the Asterisk/Teams side of the integration.

After editing the configuration, enable and start OpenSIPS, then verify that it is listening on the expected port.

```
systemctl enable --now opensips
ss -lntp | grep 5091
ss -lntp | grep 5067
```

Asterisk Teams Configuration

Create a dedicated PJSIP TLS transport for Teams. Keep it separate from the normal PJSIP TLS transport used by phones. The example below uses port 5091 and a dedicated endpoint named `msteams_trunk_from_teams`.

```
[transporttls]
type=transport
protocol=tls
bind=0.0.0.0:5091
cert_file=/etc/opensips/ssl/cert.crt
ca_list_file=/etc/opensips/ssl/ca.crt
priv_key_file=/etc/opensips/ssl/privkey.crt
cipher=ECDHE-RSA-CHACHA20-POLY1305,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-AES128-GCM-
SHA256,ECDHE-RSA-AES256-SHA384,ECDHE-RSA-AES128-SHA256,AES256-GCM-SHA384,AES128-GCM-SHA256
method=sslv23
external_media_address=<PUBLIC-ASTERISK-IP>
external_signaling_address=<PUBLIC-ASTERISK-IP>

[msteams_trunk_from_teams]
```

```
type=endpoint
transport=transporttls
context=msteams
disallow=all
allow=ulaw
aors=aor_msteams_trunk_from_teams
media_encryption=sdes
from_domain=<ASTERISK-FQDN>
send_pai=no
rewrite_contact=no
force_rport=no
sdp_owner=-
sdp_session=FullysPBX
allow_transfer=yes
ice_support=no
direct_media=no
timers_sess_expires=3600
;session_timers=accepted
;session_expires=3600

[aor_msteams_trunk_from_teams]
type=aor
qualify_frequency=60
contact=sip:<OPENSIPS-FQDN>:5067

[msteams_trunk_from_teams]
type=identify
endpoint=msteams_trunk_from_teams
match=<PUBLIC-ASTERISK-IP>
```

Update `sorcery.conf` so realtime PJSIP objects and static configuration sections can coexist. This allows MiRTA PBX realtime objects to continue working while the Teams transport, AOR, and identify sections are read from static configuration.

```
[res_pjsip]
endpoint=realtime,ps_endpoints
endpoint=config,pjsip.conf,criteria=type=endpoint

auth=realtime,ps_auths
```

```
aor=realtime,ps_aors
aor=config,pjsip.conf,criteria=type=aor

domain_alias=realtime,ps_domain_aliases

contact=realtime,ps_contacts

[res_pjsip_endpoint_identifier_ip]
identify=realtime,ps_endpoint_id_ips
identify=config,pjsip.conf,criteria=type=identify

[res_pjsip_publish_asterisk]
asterisk-publication=realtime,ps_asterisk_publications

[res_pjsip_outbound_publish]
outbound-publish=realtime,ps_outbound_publishes

[res_pjsip_pubsub]
inbound-publication=realtime,ps_inbound_publications
```

Reload PJSIP only after the certificate files exist and the transport can bind to the configured port.

```
asterisk -rx "pjsip reload"
asterisk -rx "pjsip show transports"
asterisk -rx "pjsip show endpoint msteams_trunk_from_teams"
```

Certificate Generation

The certificate must include the public names used by the Teams SBC and related Asterisk/OpenSIPS domains. The following example writes the certificate files where the OpenSIPS and PJSIP examples expect them.

```
./acme.sh --issue --keylength 4096 --standalone \
  -d asterisk.example.com \
  -d opensips.example.com \
  -d teams1.example.com \
  --fullchain-file /etc/opensips/ssl/cert.crt \
  --cert-file /etc/opensips/ssl/ca.crt \
  --key-file /etc/opensips/ssl/privkey.crt \
```

```
  --server https://acme-v02.api.letsencrypt.org/directory
```

If acme.sh is not installed yet, install it first and then rerun the certificate request with the real contact email and domain names.

```
curl https://get.acme.sh | sh -s email=support@example.com
```

MiRTA PBX Teams Configuration

In **Admin > Settings**, locate the **MS Teams integration** section. Enable the integration, set the OpenSIPS socket, and select or enter the server where OpenSIPS is running.

In **Admin > Tenants**, edit the tenant and set the Microsoft Teams address/name assigned to the Teams connection, for example `sbc.example.com`.

If Teams presence checks are required, also store the Microsoft tenant ID in the tenant configuration.

MiRTA PBX Teams Extension Configuration

MiRTA PBX connects a Teams user by using a custom extension. The custom extension represents the external Teams number while still participating in PBX routing and status logic.

1. Create or edit the custom extension for the Teams user.
2. Open the extension security section.
3. Set the authentication type to **Use Microsoft Teams**.
4. Set the authentication caller ID to the phone number assigned to the Teams user.
5. Save the extension and test inbound and outbound calls with a single Teams user before repeating the configuration for others.

Presence and Status Integration

Teams does not expose extension state to MiRTA PBX in the same way as a SIP phone. MiRTA PBX can still check the Teams extension state before dialing a Teams extension, which helps avoid sending a PBX call to a Teams user who is already busy in Teams.

1. In **Admin > Tenants**, fill the Microsoft tenant ID.
2. In the custom extension, fill the Teams extension ID.
3. In **Configuration > Settings**, fill the Microsoft client ID and client secret used for the status lookup.
4. Open **Status > Peers** and verify that MiRTA PBX shows the state for the custom extension and the related Teams extension.

Debugging and Validation

OpenSIPS Listener

Confirm OpenSIPS is listening on the expected Teams/PBX ports.

```
ss -lntp | grep -E "5067|5091"
netstat -nap | grep 5091
```

Teams Connectivity

In the Teams admin center, check whether the SBC becomes active after OpenSIPS, certificates, and Asterisk PJSIP are running. Also confirm that Teams SIP OPTIONS are enabled for the SBC.

Asterisk PJSIP

Verify the Teams transport and endpoint from the Asterisk CLI.

```
asterisk -rx "pjsip show transports"
asterisk -rx "pjsip show endpoint msteams_trunk_from_teams"
asterisk -rx "pjsip show aor aor_msteams_trunk_from_teams"
```

Call Testing

- Place an outbound call from the Teams user through MiRTA PBX and check Asterisk logs for the `msteams` context.
- Place an inbound call from MiRTA PBX to the Teams custom extension and confirm caller ID and media.

- Review **Status > Peers** after configuring the Microsoft tenant ID, Teams extension ID, client ID, and client secret.

Operational Notes

- Keep the Teams PJSIP transport separate from phone transports to avoid changing phone registration behavior.
- Use descriptive DNS names for the Teams SBC and include all required names in the certificate.
- Validate Microsoft licensing and Direct Routing policy assignment before troubleshooting MiRTA PBX routing.
- If the SBC remains inactive in Teams, check DNS, certificate chain, SIP OPTIONS, OpenSIPS listener state, and Asterisk PJSIP transport binding.

Revision #6
Created 2026-06-02 21:59:15 UTC by Admin
Updated 2026-06-06 22:22:32 UTC by Admin