Lightwire's Teams Phone Configuration Guide for Office 365 Administrators

This document is designed to provide an overview of the steps required to successfully configure a Teams instance for use with Lightwire's SIP services. Lightwire sees Teams as a third-party PBX and as such does not get involved in the configuration on the Microsoft side.

Teams configuration happens in three parts, core tenancy setup of the phone system, the per-user configuration and then the setup for Auto Attendants and Calling Queues.

This document provides all the detail we believe is necessary to successfully implement the first two parts when followed by a qualified systems engineer—Auto Attendants and Calling Queues configuration and design is up to you.

Contents

Licencing 2
Phone System Licencing 2
Part 1 - Core Tenancy Configuration 3
Adding our Siphosting calling domain to the Office 365 Tenancy 3
Configuring the PSTN Gateway in the Office 365 Tenancy..... 4
Adding a temporary licenced admin user..... 4
Connection to Office 365 with PowerShell 5
Create the PSTN gateway 7
Configure PSTN Usage..... 8
Core Office 365 Tenancy configuration complete 8
Part 2: Enabling a user and assign a routing policy 9
Enabling voice, voice mail and assigning the phone number. 9
Allowing calling and assigning the voice routing policy..... 9
Part 3: Resource Accounts.....10
Assigning a phone number to an Auto Attendant or Call Queue.....10

Licencing

Phone System Licencing

The Lightwire Microsoft Teams Phone package provides you with the ability to make and receive phone calls between your Microsoft Teams tenancy and the PSTN.

Microsoft 365 Business Standard licenses require the “Microsoft Teams Phone Standard” add-on. Microsoft also offer a “Teams Phone with Calling Plan” add-on; this is incompatible with Lightwire calling.

Enterprise users require the Microsoft Teams Phone Standard license add-on. This is additional for Microsoft Office 365 Enterprise E1, or E3 licenses, and included in Office 365 Enterprise E5 licence.

Microsoft Office 365 licenses are purchased separately from within your Office 365 tenancy, or from your Microsoft licensing provider.

Each user requiring access to calling requires a Microsoft Teams Phone Standard licence which is an additional cost to the Lightwire Teams SIP trunk channel package.

Part 1 - Core Tenancy Configuration

Adding our Siphosting calling domain to the Office 365 Tenancy

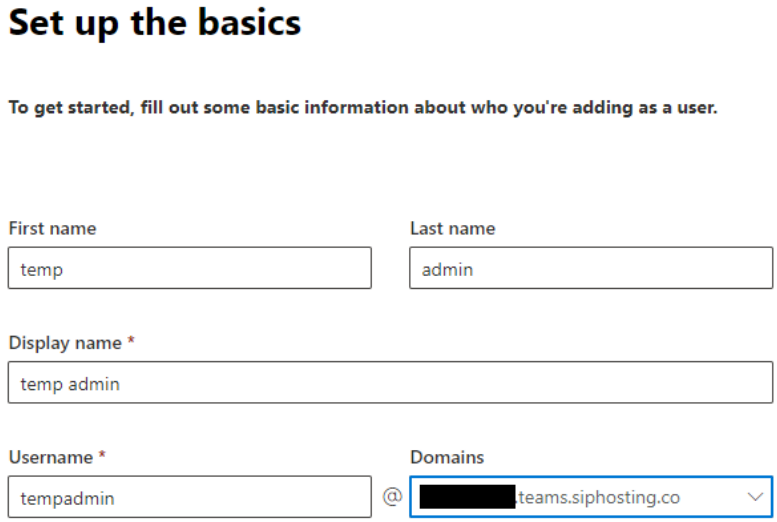
1. During provisioning, Lightwire will allocate and send the nominated technical contact a new unique Fully-Qualified Domain Names (FQDN's) which will resolve to our Teams Calling Session Border Controllers (SBC's).
   a. The address will be in the form of ***customername*.teams.siphosting.co**
2. You will need to add the Domain Names into the Office 365 Tenancy that they are configuring for Teams Calling by following the Microsoft Add a domain to Office 365 guide (available at https://docs.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide).
3. During setup Office 365 will display a TXT VALUE such as 'MS=865412465' to verify ownership of this domain. You will need to provide us with this value.
4. Lightwire will add TXT DNS records to allow the customer to verify the domains in the Office 365 tenant.
5. Once notified by Lightwire that the TXT record has been published in our Public Zone, you can proceed with the setup and verify the domain in Office 365.
6. Please leave all the online services (e.g. Exchange, Skype for Business, Mobile Device Management) unchecked.
7. Once set up successfully, the status of the domain should read "Setup Complete."

Prerequisites and connecting to your Office 365 Tenancy

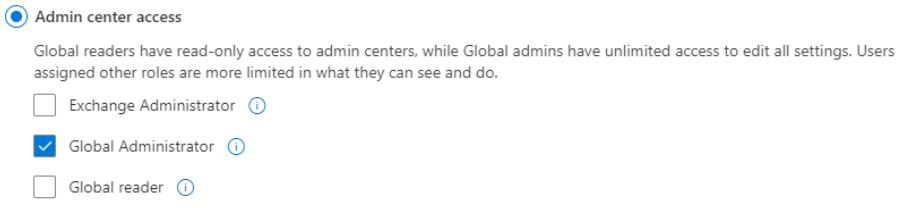
Adding a temporary licenced admin user

In order for 365 to allow for the Direct Routing FQDN to be created as a PSTN gateway a user needs to be created temporarily using the domain. This user requires a office 365 and Microsoft Teams Phone Standard license. If you don't have a spare set, the Office 365 Enterprise E5 trial can be added to your tenancy and assigned to this user.

1. In the Microsoft 365 admin centre (https://admin.microsoft.com) create a new user: Users > Active Users > Add a User. Name this temporary user how you wish, and ensure the domain selected is the Lightwire provided FQDN



2. Assign an Office 365 E1 or E3 license, and a Microsoft Teams Phone Standard license, or an Office 365 E5 license to this user
    a. Note: This license will not be permanently used. Once the Direct Routing gateway is created the user can be removed and the license relinquished
    b. Also note: Microsoft Teams Phone Standard – Virtual User licenses do not allow for this process as they are only used for resource accounts.
3. Assign Global Administrator to this user

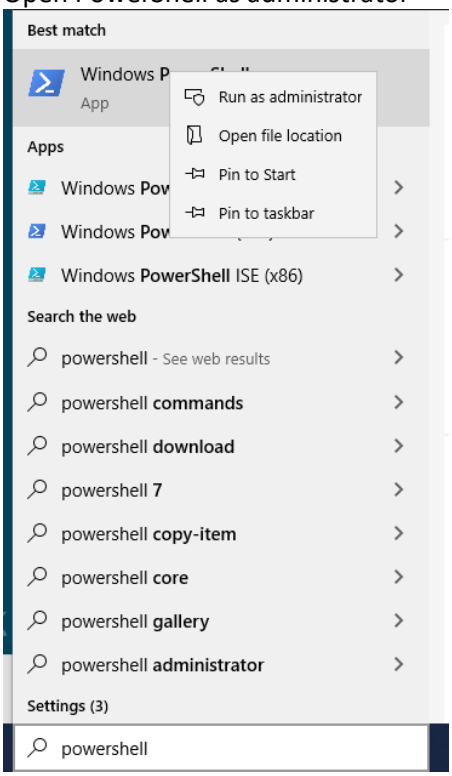


4. Finish adding. There may be a wait of up to a few hours for this to propagate and allow for the next step to be completed.

Connection to Office 365 with PowerShell

Note for the following your user should be a Global Administrator or have the correct permissions delegated to complete the configuration in the guide.

1. Open PowerShell as administrator

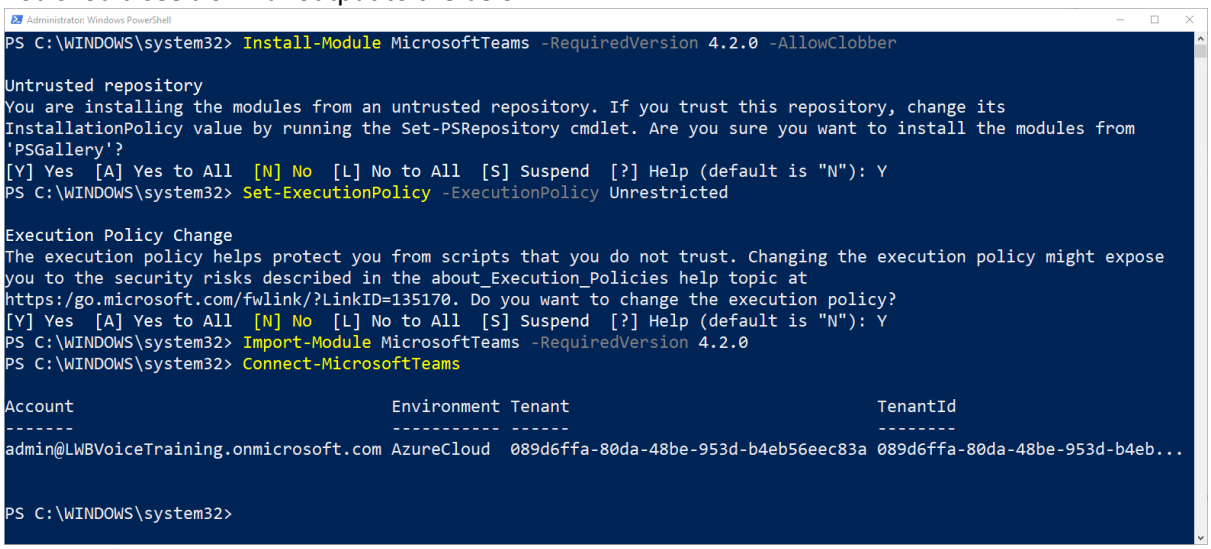


2. Paste the following four commands into the Powershell terminal:

```
Install-Module MicrosoftTeams -RequiredVersion 4.2.0 -AllowClobber
Set-ExecutionPolicy -ExecutionPolicy Unrestricted
Import-Module MicrosoftTeams -RequiredVersion 4.2.0
Connect-MicrosoftTeams
```

Accept the options when you are prompted

You should see a similar output to the below:



3. You'll be prompted to log in. Use your Global Admin login credentials for the Office 365 tenancy
    a. In the **Sign in** to your account dialogue box, type your Teams Online administrator password, and then click **Sign in**.
    b. Follow the instructions in the **Sign in to your account** dialogue box to provide any additional authentication information, such as a verification code, and then click **Verify**.

More information on connecting to and managing Microsoft Teams with Powershell is available here: https://docs.microsoft.com/en-us/microsoftteams/teams-powershell-install

If you have already installed a previous version of the MicrosoftTeams Powershell module, you can upgrade to the latest recommended version using the below command:

```
Update-Module MicrosoftTeams -RequiredVersion 4.2.0
```

www.lightwirebusiness.co
NZ: South Bloc Building Level 2, 19 Knox Street, Hamilton, New Zealand | 0800 534 567
AU: 11th floor, 9 Lawson Street, Southport, Australia | 1300 016 678

Configuring the PSTN Gateway in the Office 365 Tenancy

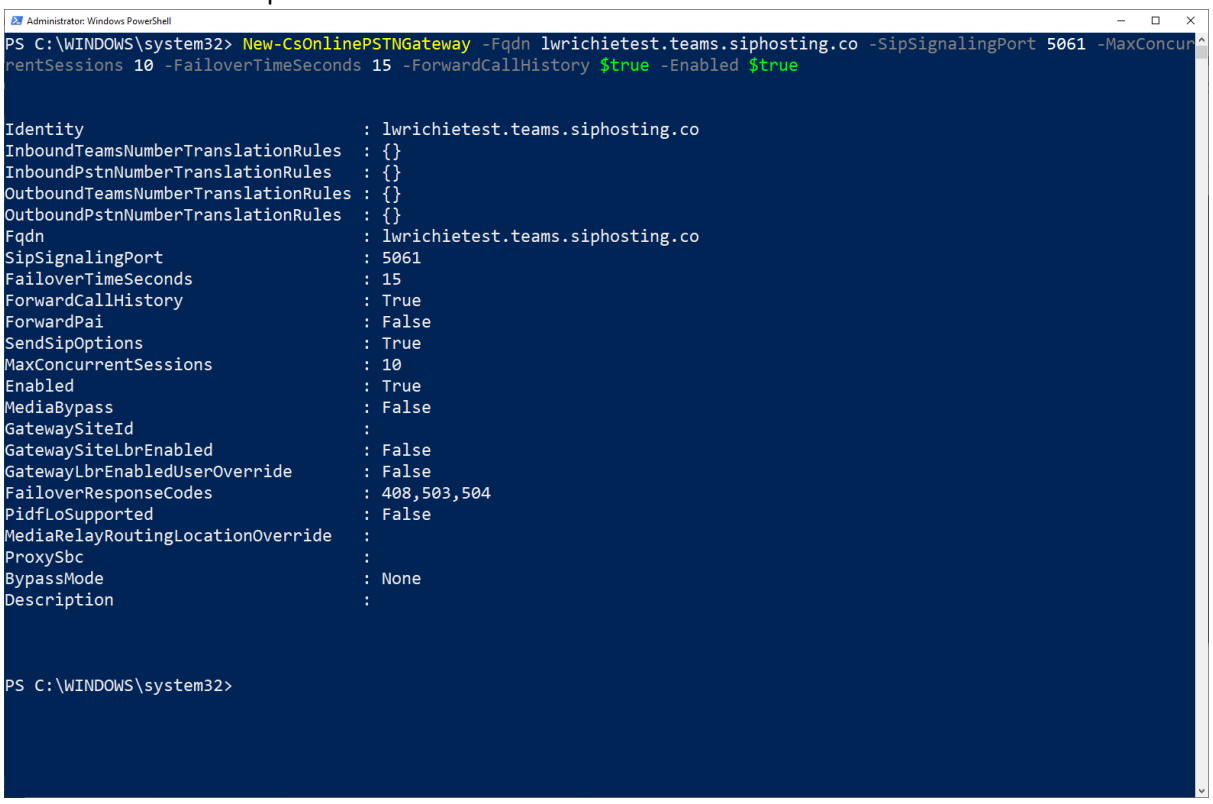
Create the PSTN gateway

Enter the below command into Powershell, replacing “customername” with your own (from the provided FQDN). Also ensure that MaxConcurrentSessions is greater than or equal to the number of voice channels purchased from Lightwire (ie if you have purchased 20 voice channels, please ensure that this is set to 20 or more).

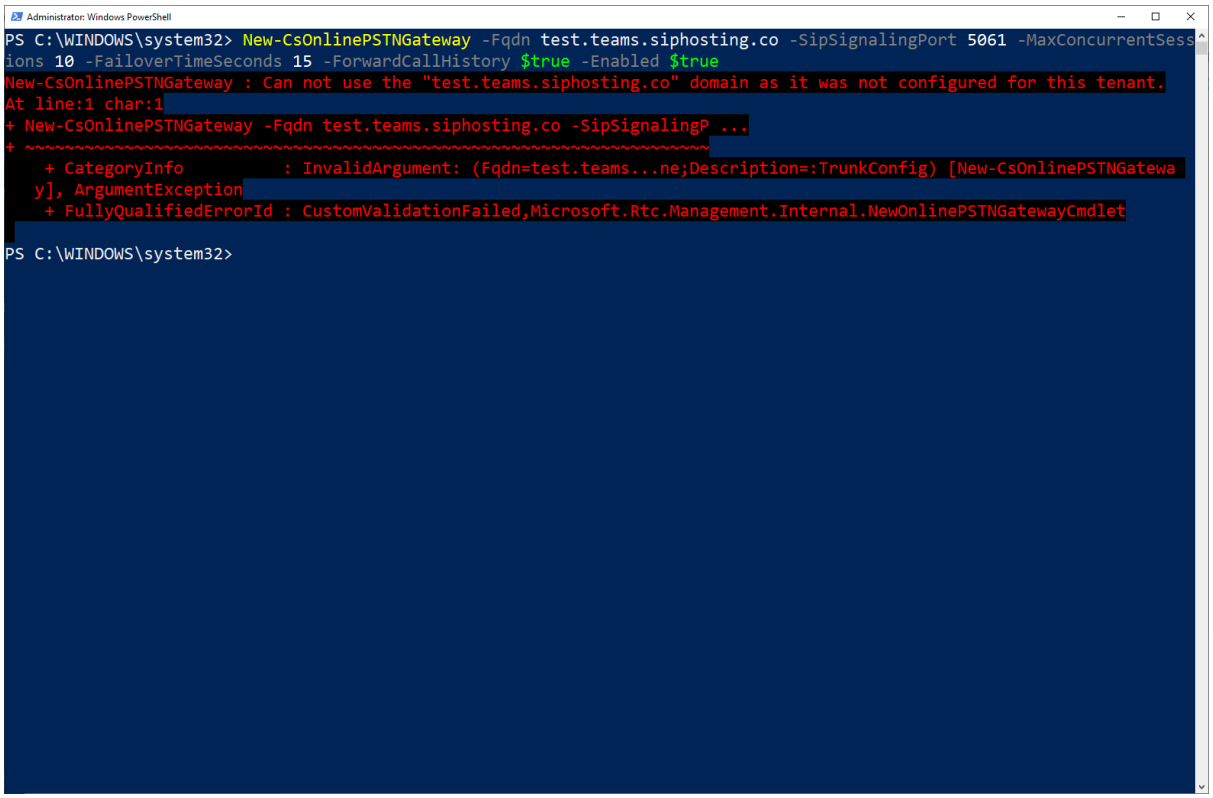
Please note, this is a single command, and needs to be entered without a line break

New-CsOnlinePSTNGateway -Fqdn **customername.teams.siphosting.co** -SipSignalingPort 5061 -MaxConcurrentSessions 10 -FailoverTimeSeconds 15 -ForwardCallHistory $true -Enabled $true

You should see an output similar to the below:



If you receive an error as below, please check to ensure that you have entered the FQDN correctly in the first instance. If you have only just added the global admin user in the previous step you may need to wait a short time before proceeding.



Configure PSTN Usage

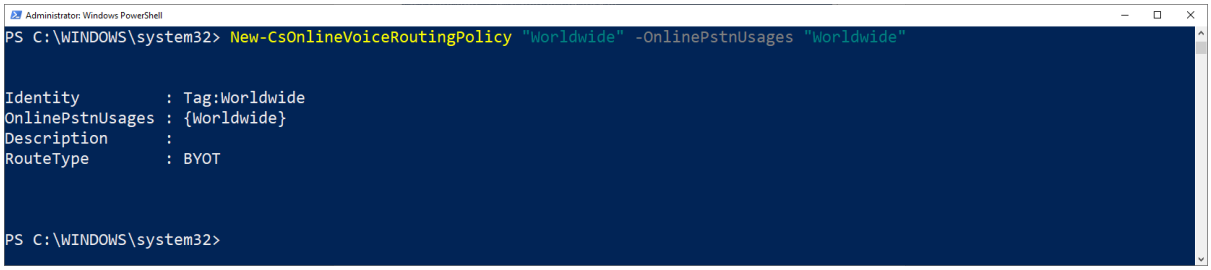
Add a new PSTN Usage called “Worldwide” and add it to the “Global” identity:

```
Set-CsOnlinePstnUsage -Identity Global -Usage @{Add=”Worldwide”}
```

Create Voice Routing Policy

Create a new Voice Routing Policy and add the PSTN usage to this:

```
New-CsOnlineVoiceRoutingPolicy “Worldwide” -OnlinePstnUsages “Worldwide”
```

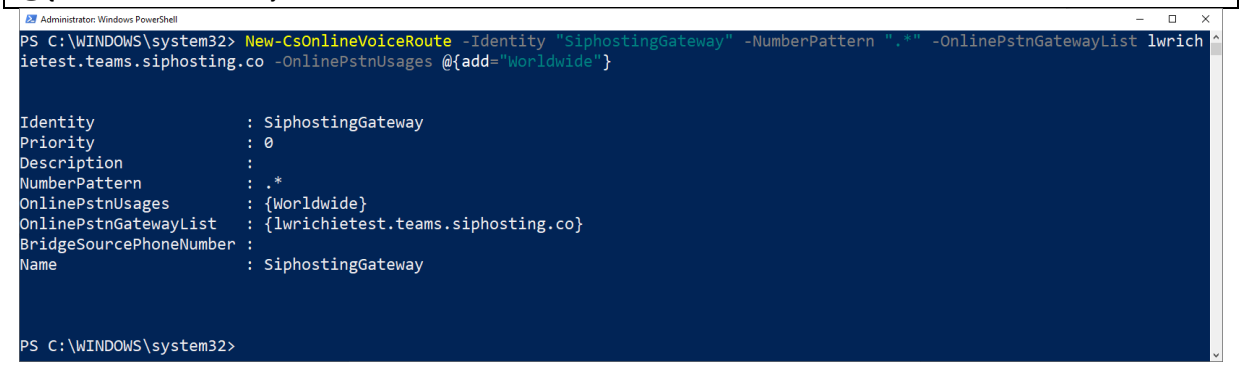


Create Voice Routes

Create a new voice route that routes all calls to the SBCs, and adds it to the PSTN usage created above:

Please note, this is a single command, and needs to be entered without a line break.

```
New-CsOnlineVoiceRoute -Identity “SiphostingGateway” -NumberPattern “.*”
-OnlinePstnGatewayList customername.teams.siphosting.co -OnlinePstnUsages
@{add="Worldwide"}
```



Note: customername.teams.siphosting.co need to be modified to match the FQDN provide in **Step 1.**

The -Identity “SiphostingGateway” is customisable, e.g. you could call it -Identity “MyCompanyNameGateway”

Core Office 365 Tenancy configuration complete

You have now completed the configuration requirements you can now exit out of the PowerShell Session.

```
Exit-PSSession
```

Part 2: Enabling a user and assign a routing policy

Either enable a test user, or use an existing user. Ensure that the user has a Microsoft Teams Phone Standard license. These commands will fail if the user does not have the appropriate license.

Enabling voice, voice mail and assigning the phone number.

Open Powershell as admin (per page 5) and run the following command:

```
Connect-MicrosoftTeams
```

Log in using your Microsoft 365 admin credentials when prompted.

Run the below, replacing “username@customerdomain.com” with the required username. Also replace the phone number with the number to be assigned to this user.
Please note, this is a single command, and needs to be entered without a line break

```
Set-CsPhoneNumberAssignment -Identity user.name@customerdomain.com -PhoneNumber +645555555 -PhoneNumberType DirectRouting
```

To enable voice for a user who does not require a direct dial phone number, use the following command, replacing “username@customerdomain.com” with the required username.

```
Set-CsPhoneNumberAssignment -Identity user.name@customerdomain.com -EnterpriseVoiceEnabled $true
```

Allowing calling and assigning the voice routing policy.

Grant the “AllowCalling” policy to the user (replacing the example address):

```
Grant-CsTeamsCallingPolicy -PolicyName AllowCalling -Identity user.name@customerdomain.com
```

Grant the following policy to the user:
Please note, this is a single command, and needs to be entered without a line break

```
Grant-CsOnlineVoiceRoutingPolicy -Identity user.name@customerdomain.com -PolicyName “Worldwide”
```

Part 3: Resource Accounts

For more on Auto Attendances and Call Queues in Microsoft Teams, please see the relevant documentation on the Microsoft knowledge base

- Auto Attendants: https://docs.microsoft.com/en-us/microsoftteams/create-a-phone-system-auto-attendant
- Call Queues: https://docs.microsoft.com/en-us/microsoftteams/create-a-phone-system-call-queue
- Managing Resource Accounts: https://docs.microsoft.com/en-us/microsoftteams/manage-resource-accounts

A Resource Account requires a free Microsoft Teams Phone Standard – Virtual User license.

Assigning a phone number to an Auto Attendant or Call Queue

Lightwire Microsoft Teams Calling phone numbers can only be assigned to resource accounts using Powershell. To assign a number:

Open Powershell as admin (per page 5) and run the following command:

```
Connect-MicrosoftTeams
```

Log in using your Microsoft 365 admin credentials when prompted.

Run the below command replacing user.name@domain.com with the username you'd assigned to the resource account, and the phone number with one provided by Lightwire.
Please note, this is a single command, and needs to be entered without a line break

```
Set-CsPhoneNumberAssignment -Identity user.name@customerdomain.com -PhoneNumber +645555555 -PhoneNumberType DirectRouting
```

www.lightwirebusiness.co
NZ: South Bloc Building Level 2, 19 Knox Street, Hamilton, New Zealand | 0800 534 567
AU: 11th floor, 9 Lawson Street, Southport, Australia | 1300 016 678

Technical Notes

Issue:

Some networks provide Anonymous calls as the FROM field within SIP. Teams will translate the word Anonymous to numbers as if it's an alphanumerically dialled number. This will show the call coming from 266696687 within Teams.

Resolution:

We'd recommend Office 365 administrators add 266696687 as a contact called "Anonymous" within the address book. This will avoid an "Unknown Contact" with the number 266696687 showing in Call Histories confusing end users.

Issue:

You wish to enable 1-to-1 recording of calls in Microsoft Teams

Resolution

This can be enabled for users with the following PowerShell command:

```
Set-CsTeamsCallingPolicy -Identity Global -AllowCloudRecordingForCalls $True
```

This will enable users to start recording their calls from the call window in the same way that meetings can be recorded. When the call ends the recording will be made available in their OneDrive

Please note that when activated an automated message plays to the other party to inform them that the call is now being recorded.

Issue

Users who do not have a direct dial phone number assigned to them present their outbound calls as "Anonymous". This may impact outbound calling to some carriers.

Resolution

Lightwire can mask all anonymous outbound calling with a single number. Please request this if required.

If you have numbers assigned to resource accounts, used for Auto Attendants or Calling Queues, you can set Caller ID Policies yourself. This provides more flexibility as you can set these up on a per-user basic. To set this up:

1. Create a new policy. You can change the "Identity" to any name if you require multiple policies. The description can be set as required as well.

```
New-CsCallingLineIdentity  -Identity MaskOutbound -Description "Mask outbound calls with the reception DDI"
```

2. Set a variable to retrieve details from the required resource account. The variable name ($ResourceAccount1 in the below example) can be modified per your requirements. Ensure that you replace resourceaccount@domain.com with the UPN of the resource account you're wanting to mask with.

```
$ResourceAccount1 = Get-CsOnlineApplicationInstance -Identity resourceaccount@domain.com
```

3. Create the calling policy, ensuring that the Identity is the one set up in step 1 above, and you use the variable set in step 2

```
Set-CsCallingLineIdentity -Identity MaskOutbound -CallingIDSubstitute resource -ResourceAccount $ResourceAccount1.ObjectId
```

4. Assign the policy to users, ensuring that user@domain.com is updated to reflect the user's account details

```
Grant-CsCallingLineIdentity -Identity user@domain.com -PolicyName MaskOutbound
```