Apresa - Configuration of Teams for recording

Introduction

This document describes the steps to prepare and configure Teams to record calls of users.

Prerequisites

To do recording, you will need access to a running instance of the Teams Recorder Bot for Apresa. In this document we will assume the bot is already set up and available. You will need to know the application ID of the bot.

The commands to configure Teams are done in the PowerShell of Windows. You will need an administrator account of your Microsoft subscription to perform the actions. The commands will use the Skype for Business online connector PowerShell module. If you do not have this installed yet, please see:

https://www.microsoft.com/en-us/download/details.aspx?id=39366

Starting a Teams configuration session

Open Windows PowerShell (click Windows key and type powershell), and execute the following commands:

- `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope Process`
- `Import-Module SkypeOnlineConnector`
- `$userCredential = Get-Credential`
- `$sfbSession = New-CsOnlineSession -Credential $userCredential -Verbose`
- `Import-PSSession $sfbSession`

The previous commands will be needed each time you do a configuration change in a new PowerShell session.

If you are prompted later for credentials, it might be a time-out has occurred. It is then recommended that you close PowerShell, and open a fresh new one, and initialize it again with the commands above.

Creating a reference to the recorder bot

Continuing the same PowerShell session, in the following command we will create a reference to the Teams Recorder Bot that we will use to record calls.

- ⚠ **Anything between <…> needs to be replaced and filled in. Remove the < >.**

In the command below, there are three things to replace and fill in. The recorder email address can be anything and does not need to exist. The recorder name can be freely chosen. The bot application ID must reference the existing Teams Bot application that you want to use.

- `New-CsOnlineApplicationInstance -UserPrincipalName <recorder@company.com> -DisplayName <RecorderName> -ApplicationId <botApplicationId>`

The system will reply and output on the screen a new object id of the created object. We will need to use this object id in the next command and further commands.

- `Sync-CsOnlineApplicationInstance -ObjectId <objectId>`

Granting access to the recorder bot

The tenant admin needs to give permission to the Vidicode Bot to access data. This can be done using this link. Fill in the bot application ID, then visit the link using a browser. You will be asked to login as administrator.

https://login.microsoftonline.com/common/adminconsent?client_id=<botApplicationId>

After granting permission, there can be an error regarding a lack of return address. This error can be ignored.

Creating a recording policy

A recording policy describes to Teams which recording bot should be used. This policy can then be assigned to a user in a later step.

The policy description and policy identifier can be freely chosen. The policy identifier is recommended to be a short identifier with no spaces. We will need to reference it later. The objectid must be filled in with the object id that was created earlier.

- `New-CsTeamsComplianceRecordingPolicy -Enabled $true -Description "<policyDescription>" <policyIdentity>`
- `Set-CsTeamsComplianceRecordingPolicy -Identity <policyIdentity> ComplianceRecordingApplications ` @(New CsTeamsComplianceRecordingApplication -Parent <policyIdentity> -Id <objectId>)`

For verification, you can retrieve information about the recording policy as follows. This should work after a minute.

- Get-CsTeamsComplianceRecordingPolicy <policyIdentity>

Assign a recording policy to a user

Finally, we can assign a recording policy to a user, to let calls of this user be recorded.

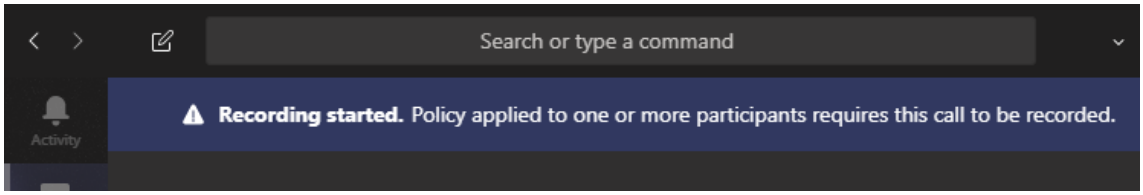
- Grant-CsTeamsComplianceRecordingPolicy -Identity userToRecord@company.com -PolicyName <policyIdentity>

⚠ **A user that has a recording policy assigned to it, will not be able to make calls if the recorder bot is not online or not functioning.**

To check what policy is assigned to a user, you can use the following command. This command will also show the Microsoft tenant ID.

- Get-CsOnlineUser <userToRecord@contoso.com> | ft sipaddress, tenantid, TeamsComplianceRecordingPolicy

After assigning a recording policy to user, it can take a few minutes for the policy to be actually applied to new calls of the user. When a call is recorded, normally a banner is displayed at the top of the Teams window of all call participants.



To no longer record calls of a user, assign a blank recording policy as follows:

- Grant-CsTeamsComplianceRecordingPolicy -Identity <userToNotRecord@contoso.com> -PolicyName ""

Configuration of the Teams Recorder Bot

Please provide the following information to the manager of the Teams Recorder Bot:

- The tenant ID (as shown in the Get-CsOnlineUser above)

If you are managing Apresa, then also provide the following information:

- Domain name of Apresa where it can be reached (https)
- Credentials for uploading recordings

Configuration of Apresa

The manager of Apresa will need the following information:

- Display names of the users that will be recorded