Technical Deployment Guide
Microsoft Teams

Kinly

kinly.com

Technical Deployment Guide
Microsoft Teams

Table of Contents

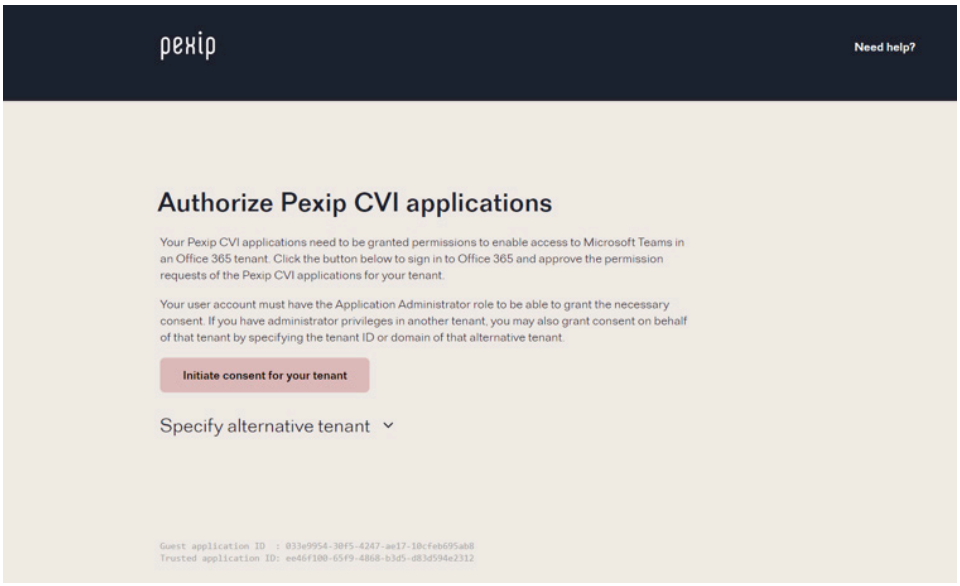
Technical Deployment Guide
Microsoft Teams

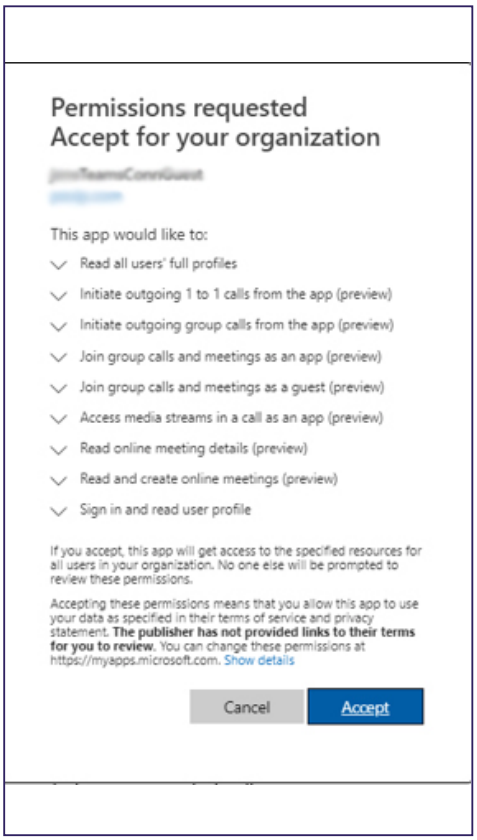
1 Customer implementation

The following section will guide you through configuring Microsoft Teams for Kinly Cloud.

1.1 Customer Teams configuration

1.11 Give consent to join Teams meetings





1 In your web browser go to **https://kcloud01-pexip-cvi-anfgs.azurewebsites.net/adminconsent/**

2 Click “Initiate consent on behalf of your own tenant”.

3 You will then be asked to verify your account. NOTE: **You must do this from an account that has Admin rights for the application to be able to grant the necessary consent.**

4 Once your account has been verified, the permissions for the Pexip Teams Guest Connector will be listed. The domain shown here is the domain where the app registration was created (this is the bot channel registration from the installation script) – it does not have to be the same as the Azure AD domain where the Teams users are homed, but for most enterprises it will be.

5 You will then be directed to select the account again in order to sign the Pexip Teams Trusted Connector.

6 The same list of permissions must be accepted for the Trusted Connector.

7 Once admin consent has been successfully granted, the success page will be displayed. NOTE: **We recommend saving the information shown on this page to ensure full knowledge of which apps were consented in which tenant should you have any problems in the future.**

Technical Deployment Guide
Microsoft Teams

1 Customer implementation

1.12 Authorize Trusted app to bypass Teams lobby and configure dialing instructions

1 In your web browser, go to https://www.microsoft.com/en-us/download/details.aspx?id=39366 and download **SkypeOnlinePowerShell.Exe.**

2 Once the download is complete go to the Downloads Folder on your computer and run **SkypeOnlinePowerShell.Exe. NOTE: The installation may fail if you do not have a compatible version of Microsoft Visual C++. The latest versions of Microsoft Visual C++ are available at https://support.microsoft.com/en-au/help/2977003/the-latest-supported-visual-c-downloads.**

3 Agree to the terms and **Install** the module.

4 Start a PowerShell session and run the following commands, where **<tenant_name>** needs to be the onmicrosoft.com domain for your tenant:

Import-Module SkypeOnlineConnector
$sfbSession = New-CsOnlineSession -OverrideAdminDomain "**<tenant_name>**.onmicrosoft.com"
Import-PSSession $sfbSession

This section will be provided by kinly, as it needs to be configured per customer

Shared domain of meet.call.vc:

New-CsVideoInteropServiceProvider -Name Pexip -TenantKey "**<virtual_reception_alias>**@meet.call.vc" -InstructionUri
https://sip.meet.call.vc/teams/?conf={ConfId}&ivr=**<virtual_reception_alias**>&d=meet.call.vc&test=test_call&prefix=**<customer_name>**.&w" -AllowAppGuestJoinsAsAuthenticated $true -AadApplicationIds "ee46f100-65f9-4868-b3d5-d83d594e2312"

For customer specific domain, this section needs to be created per customer.

1.13 Grant interoperability for the users in your tenant

Inside the already open Powershell session, add the following to grant user access:

All users:
Grant-CsTeamsVideoInteropServicePolicy -PolicyName PexipServiceProviderEnabled -Global

For testing purposes you can enable interop for named users by using the -Identity switch instead of -Global, for example:

Grant-CsTeamsVideoInteropServicePolicy -PolicyName PexipServiceProviderEnabled -Identity alice@example.com

2 Firewall openings

NOTE: **If you already have the Cloudroom service from Kinly Cloud, no additional firewall rules are needed to allow gateway services.**

The following firewall rules must be in place at Customer end to reach KinlyCloud gateway services to Microsoft Teams.

Technical Deployment Guide
Microsoft Teams

2 Firewall openings

2.1 Video endpoints inbound to Kinly Cloud

Protocol	SRC Ports	Dest Ports	Comment	Device
TCP	<any>	5060-5061	SIP / SIP TLS	Endpoint / call control system
TCP	<any>	33000 - 39999	H323 Q.931 / H.245	
TCP	<any>	1720	H323 (H.225 signaling)	
UDP	<any>	1719	H323 (RAS signaling)	
UDP	<any>	40000 - 49999	RTP/RTCP/RDP/DTLS/RTMP/STUN/TURN	

2.2 Video endpoints outbound from Kinly Cloud

Protocol	SRC Ports	Dest Ports	Comment	Device
TCP	33000-39999	5060-5061	SIP / SIP TLS	Endpoint / call control system
TCP	33000-39999	1720	H323 (RAS signaling)	
TCP	33000-39999	<any>	H323 Q.931 / H.245	
UDP	33000-39999	1719	H323 (RAS signaling)	
UDP	40000-49999	<any>	RTP/RTCP/RDP/DTLS/RTMP/STUN/TURN	

2.3 Skype for Business inbound to Kinly Cloud

Protocol	SRC Ports	Dest Ports	Description	Device
TCP / UDP	<any>	40000 – 49999	RTP/RTCP/RDP/DTLS/RTMP/STUN/TURN	Skype for Business system / edge
TCP	<any>	5061	SIP / TLS	
TCP	<any>	80	HTTP for avatar	

2.4 Skype for Business outbound from Kinly Cloud

Protocol	SRC Ports	Dest Ports	Description	Device
TCP / UDP	40000 – 49999	<any>	RTP/RTCP/RDP/DTLS/RTMP/STUN/TURN	Skype for Business system / edge
TCP	33000 – 39999	5061	SIP / TLS	

2 Firewall openings

2.5 WebRTC inbound to Kinly Cloud

Protocol	SRC Ports	Dest Ports	Description	Device
TCP / UDP	<any>	40000 – 49999	RTP/RTCP/RDP/DTLS/RTMP/STUN/TURN	WebRTC client
TCP	<any>	80	HTTP	
TCP	<any>	443	HTTPS	

2.6 WebRTC outbound from Kinly Cloud

Protocol	SRC Ports	Dest Ports	Description	Device
TCP / UDP	40000 – 49999	<any>	RTP/RTCP/RDP/DTLS/RTMP/STUN/TURN	WebRTC client