



TechNote: CASTEL and CyberGate

Version: 1.0.4 ENG
Date: 14-08-2025



Configure the CASTEL XELLIP Audio
Video Intercom for CyberGate

CyberGate

Microsoft Teams is the hub for team collaboration in Microsoft Office 365 that integrates people, content, conversations and tools your team needs. Via the CyberGate application that runs in Microsoft Azure you can now connect a CASTEL XELLIP Audio Video Intercom to your Microsoft Teams environment. Microsoft Teams users can answer incoming intercom calls – with 2-way audio and live video – on the Teams desktop client, Teams desk phone or Teams Smartphone app and open the door for visitors.

CyberGate is a subscription based Software-as-a-Service (SaaS) hosted in Azure. With CyberGate there is:

*no need to setup a hosting environment,
no need to download or install any software from CyberTwice or a 3rd party,
no need to install additional Virtual Machines,
no need for a Session Border Controller (SBC) or extra licenses for your existing SBC
no need for to get additional PSTN like phone numbers for your SIP intercoms.*

Note:

For instructions on how to purchase and configure the CyberGate service, see our Tech Note: 'Connect a SIP Intercom to MS Teams using the CyberGate service'. (<https://support.cybertwice.com/knowledgebase.php?article=6>).

CASTEL XELLIP Audio Video Intercom

For this document we used the CASTEL XE VIDEO 1B (from now on named 'Castel') to connect to the CyberGate service (from now on named 'CyberGate'). All other CASTEL XELLIP Audio Video intercoms will also work with CyberGate.

Follow the next steps to configure the Castel to connect it to CyberGate.

This manual also contains an Appendix: Install the CyberGate App. It describes the installation and usage of the CyberGate app for Microsoft Teams.

Use the CyberGate app for Microsoft Teams to:

- Open the door of the intercom by simply clicking on an Open-door button
- See the status of your intercom and calling the intercom from Teams by clicking on just one button
- Set your Availability status in a configured CyberGate Multi-ring group with one click

Installation of the CyberGate app for Microsoft Teams is highly recommended.

Connect the Castel

Connect the Castel to the network, power it on and open a webbrowser to its IP-address. Sign in with the configured or supplied username and password of the Castel.

When successfully signed-in successfully, the first menu shown is the System-Information menu.

The screenshot displays the CASTEL web interface. The top navigation bar includes icons for Home, System, Calls, Services, Synchronic, Users, Reports, and Maintenance. The main content area is divided into three sections:

- Station:** A tree view showing the device hierarchy: Network, Buttons, IP, Inputs (Entree 1, Entree 2), Outputs (Sortie 1, Sortie 2), and Camera.
- About the device:**

Model	XEVIDEO-1B
Software	2.0.1
Version	(20220323_15h50)
Hardware	
Version	18391830

Network : Interface Bridge

Interface Name	Bridge
Ip	192.168.160.113
MAC address	00:0E:AF:51:6B:ED
Gateway	192.168.160.1
Port status	active
Interface status	Connected via port eth1
Hostname	XE2516bed

Network : Interface eth0(Inactive) ▶

Network : Interface eth1(Inactive) ▶
- States:**
 - General:**

Label	Poste XEVIDEO-1B
State	Full Mode
Current User	castel
Current Profile	Profil 1 (ID : 1)
Supervisor Connexion	Not connected
 - Multimedia:**

Communication status	Idle
Call forward	
SIP standalone	Inactive
Incoming calls	0
Outgoing calls	0
Pending calls	0
Video Monitoring State	Inactive
 - Interface:**

Input[Entree 1]	Inactive
-----------------	----------

Navigate to the Calls menu.

Configuration sip globale +

SIP Configuration ▾

Global SIP parameters ▾

UDP SIP Port used for the station

TCP SIP Port used for the station

TLS SIP Port used for the station

Account parameters ▾

Choose transport type for this account

Disable Castel messages for DTMF commands

Enable synchronisation rtp

SIP standalone

Extension number

Audio codecs and port ▾

Audio RTP port number [7000;65535]

Not authorized

Authorized

Video codecs and port ▾

Provide the following information:

TCP SIP Port used for the station | 5060

Click the blue Save button when done.

Configuration sip globale +

SIP Configuration ▾

Global SIP parameters ▾

UDP SIP Port used for the station

TCP SIP Port used for the station

TLS SIP Port used for the station

Account parameters ▾

Choose transport type for this account

Disable Castel messages for DTMF commands

Enable synchronisation rtp

SIP standalone

Extension number

Audio codecs and port ▾

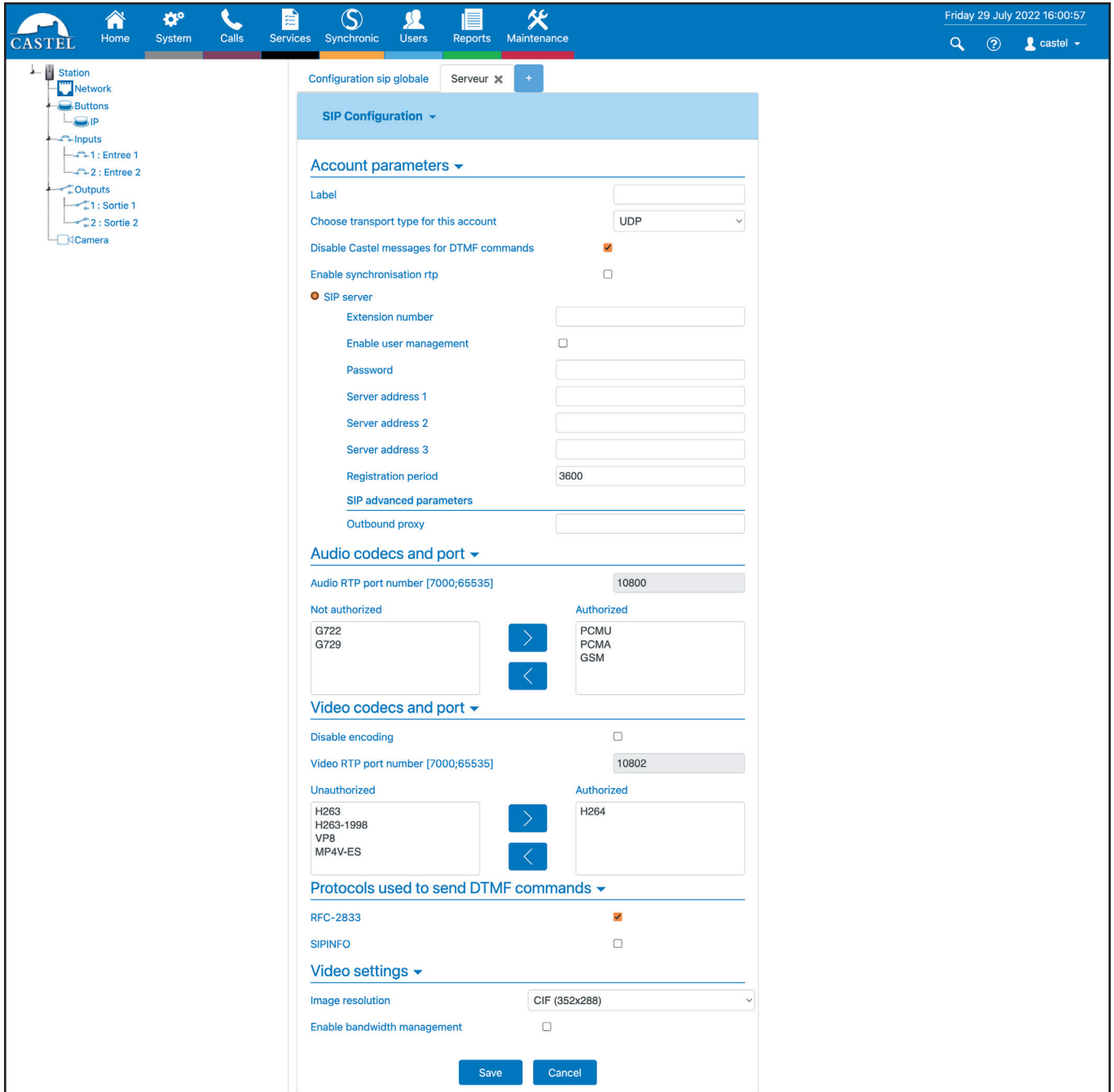
Audio RTP port number [7000;65535]

Not authorized

Authorized

Video codecs and port ▾

Click the blue '+' symbol to add the SIP server.



Provide / change the following information:

Account parameters	
Label	Label the server 'CyberGate'
Choose transport type for this account	Change to TCP
Extension number	Use the Username provided by the CyberGate Management Portal
Password	Use the Password provided by the CyberGate Management Portal

Server address 1	cybergate.cybertwice.com
Audio codecs and port	
Authorized	Only: G722
Video settings	
Image resolution	Change to HD (1280x720)

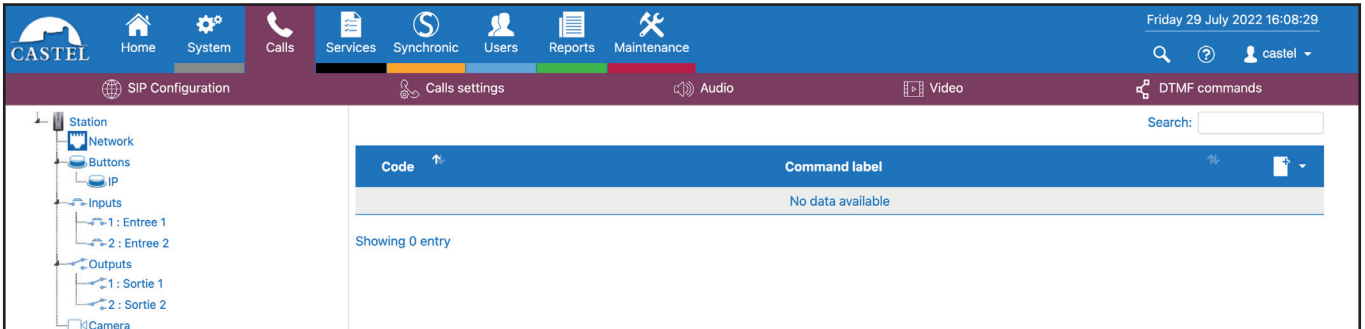
Click the blue 'Save' button when done.

The screenshot shows the CASTEL configuration interface for a SIP account named 'CyberGate'. The interface is divided into several sections:

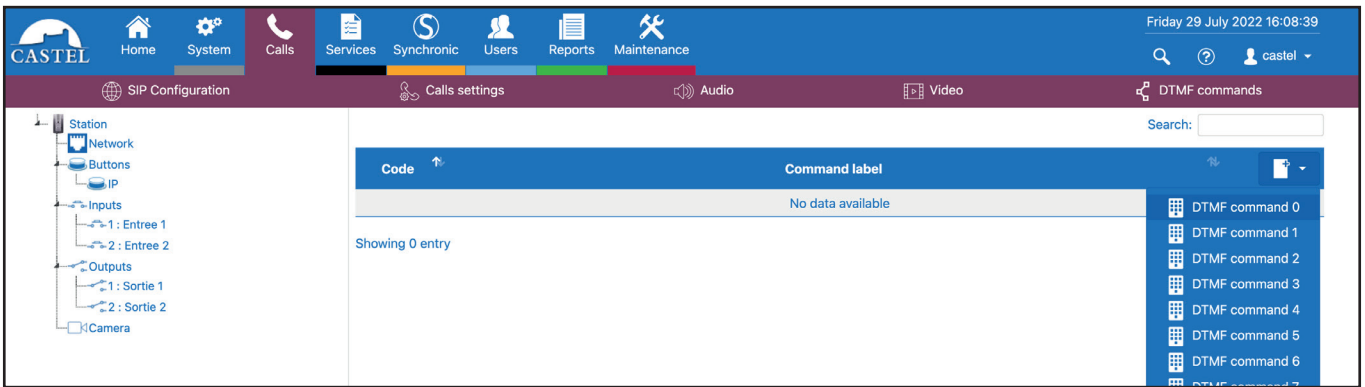
- SIP registration status:** Shows 'Registered on server(s): cybergate.cybertwice.com' with a green checkmark.
- Account parameters:**
 - Label: CyberGate
 - Choose transport type for this account: TCP
 - Disable Castel messages for DTMF commands:
 - Enable synchronisation rtp:
 - SIP server:
 - Extension number: 83YRYXUMHOKYFD7YIE99
 - Enable user management:
 - Password: [Redacted]
 - Server address 1: cybergate.cybertwice.com
 - Server address 2: [Empty]
 - Server address 3: [Empty]
 - Registration period: 3600
- Audio codecs and port:**
 - Audio RTP port number [7000;65535]: 10800
 - Not authorized: GSM, G729, PCMA, PCMU
 - Authorized: G722
- Video codecs and port:**
 - Disable encoding:
 - Video RTP port number [7000;65535]: 10802
 - Unauthorized: [Empty]
 - Authorized: H264, H263, H263-1998, VP8, MP4V-ES
- Protocols used to send DTMF commands:**
 - RFC-2833:
 - SIPINFO:
- Video settings:**
 - Image resolution: HD (1280x720)
 - Enable bandwidth management:

At the bottom of the configuration panel, there are 'Save' and 'Cancel' buttons.

Navigate to Calls - DTMF commands to configure the DTMF key to open the door.
Add a DTMF code by clicking on the '+' symbol



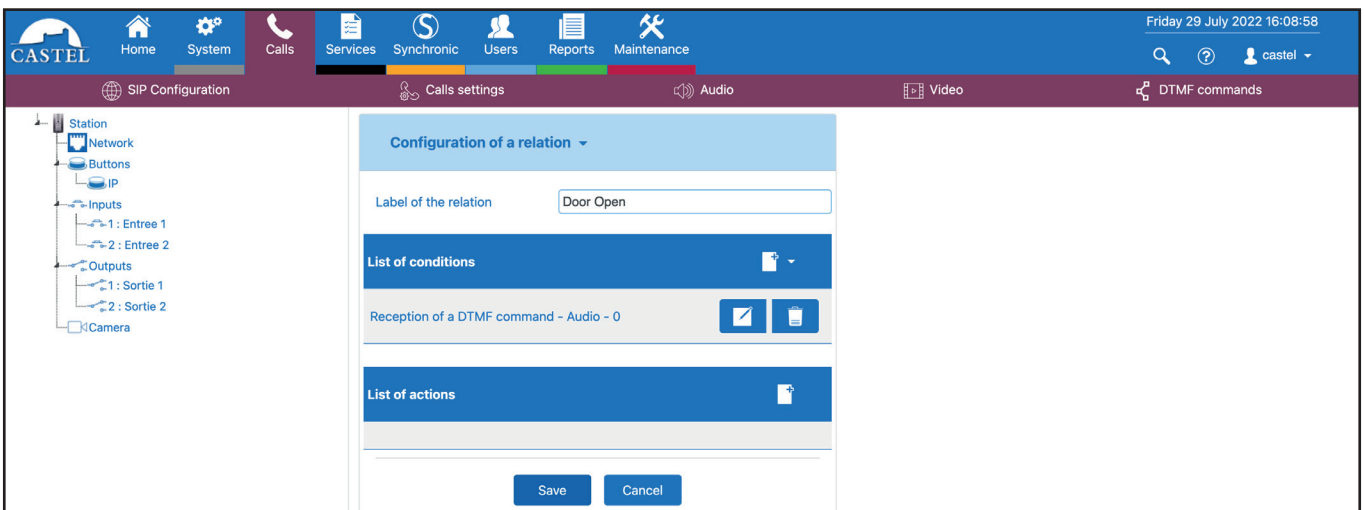
Select the DTMF command to us to open the door (in this example DTMF command 0)



Provide the following information:

Label of the relation	Label the door open action (Door Open)
-----------------------	--

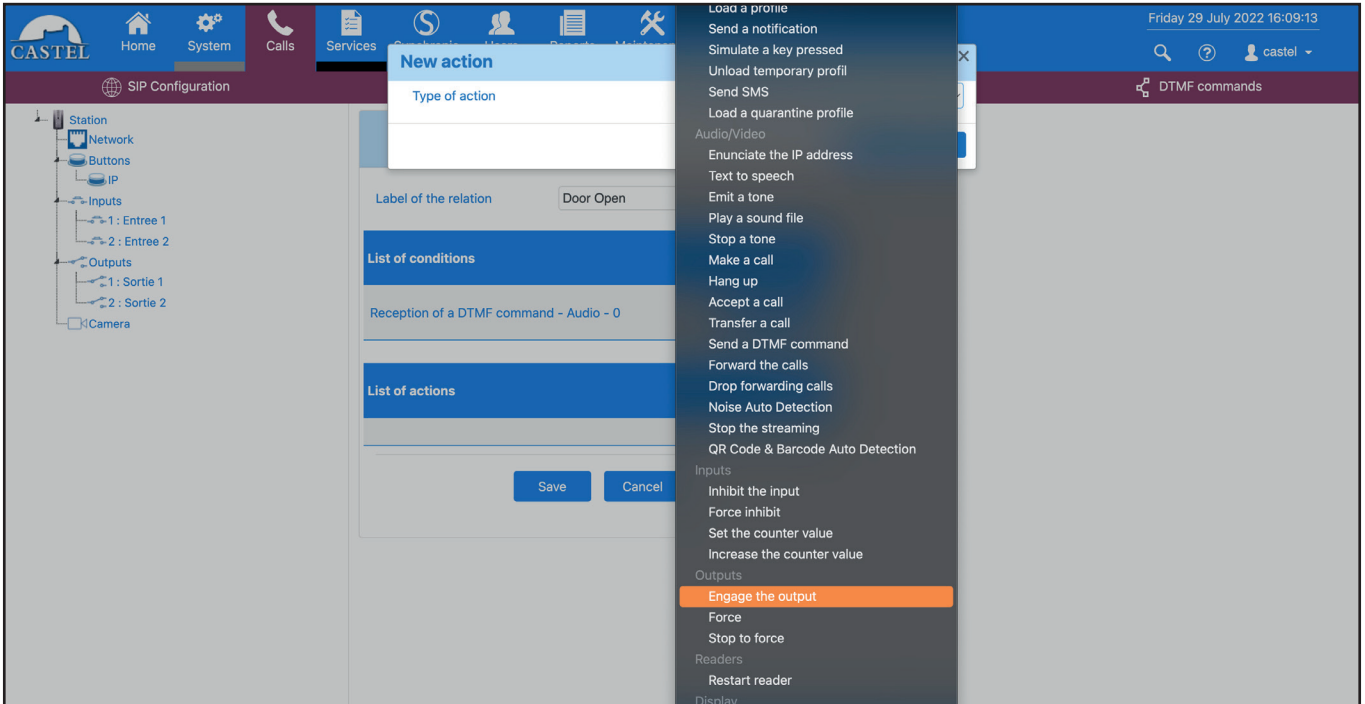
At 'List of actions', click on the '+' symbol to add the action.



C

Configuration

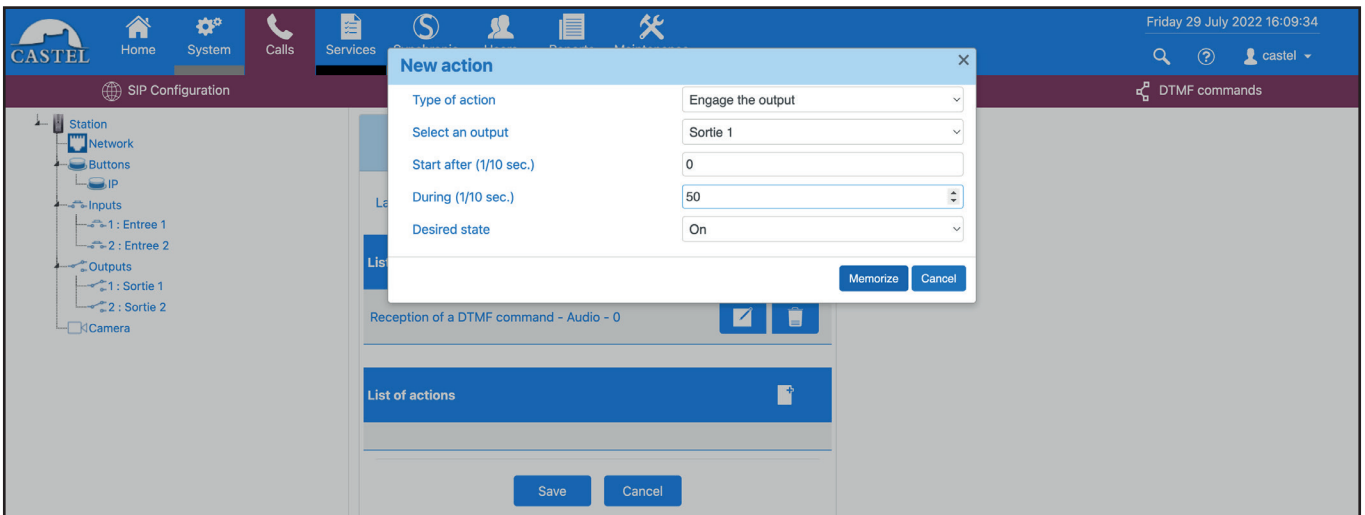
Select the 'Engage the output' action.



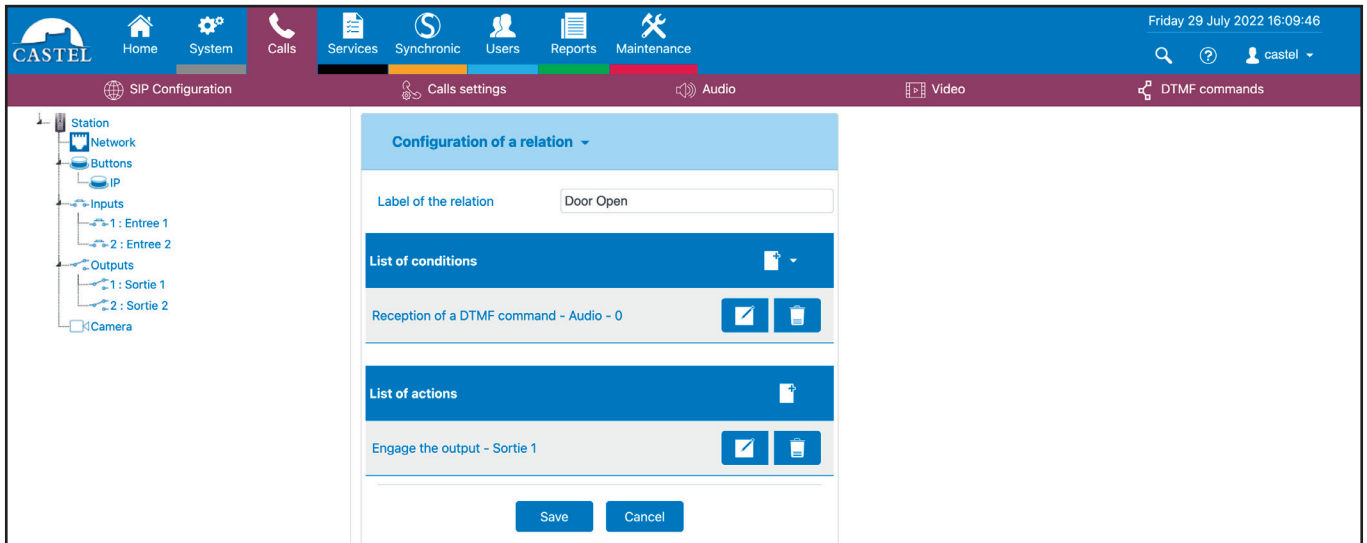
Change the following information:

During (1/10 sec.)	Change to 50 (for 5 seconds door opening) - in this example
--------------------	---

Click the blue 'Memorize' button to save the action.



Click on the blue 'Save' button to save the action.



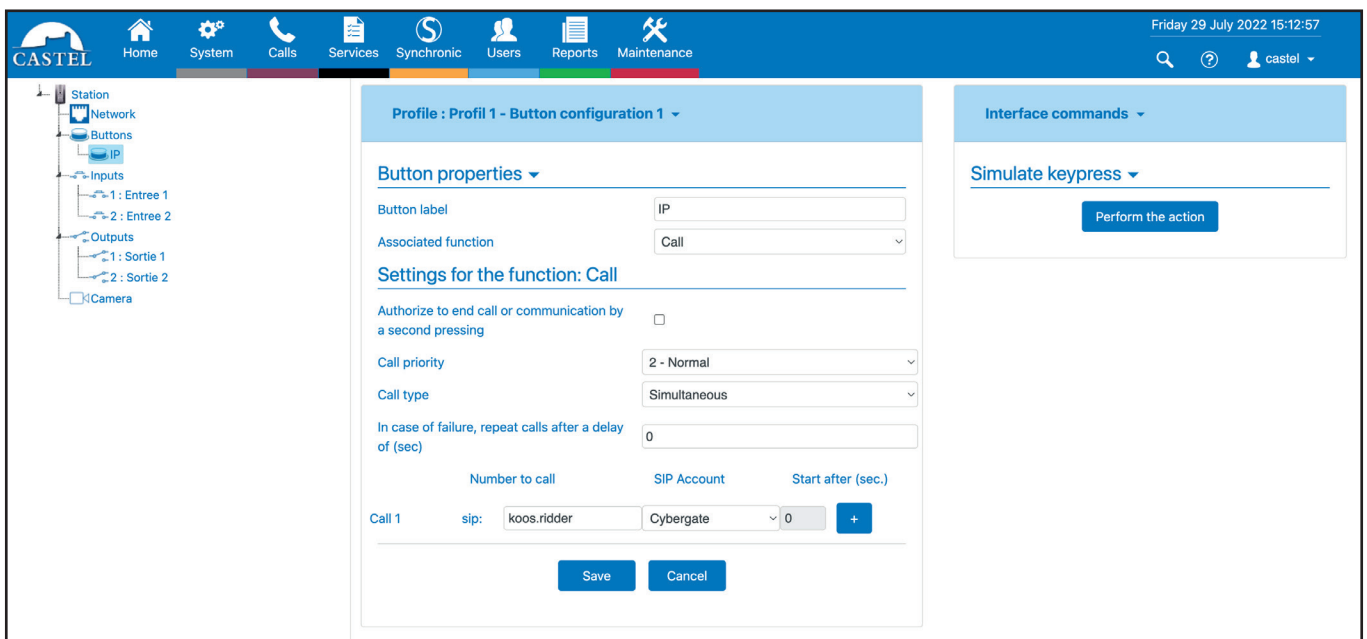
Navigate to Station-Buttons-IP (in the left column) to configure the number to dial. Provide the following information:

Call 1 sip:	Use the Teams user address without the domain part *
-------------	--

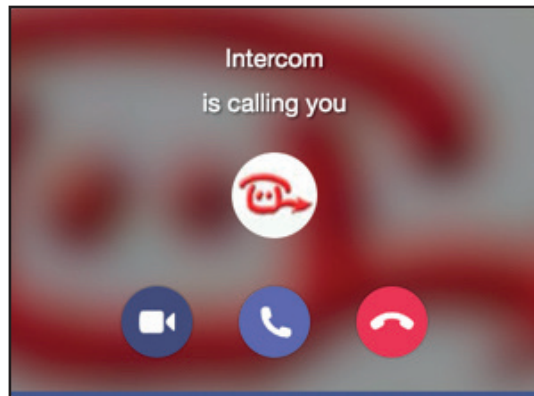
* For example, the user 'Koos Ridder, with the Teams name: *koos.ridder@mycompany.com*

will translate to this destination address:
koos.ridder

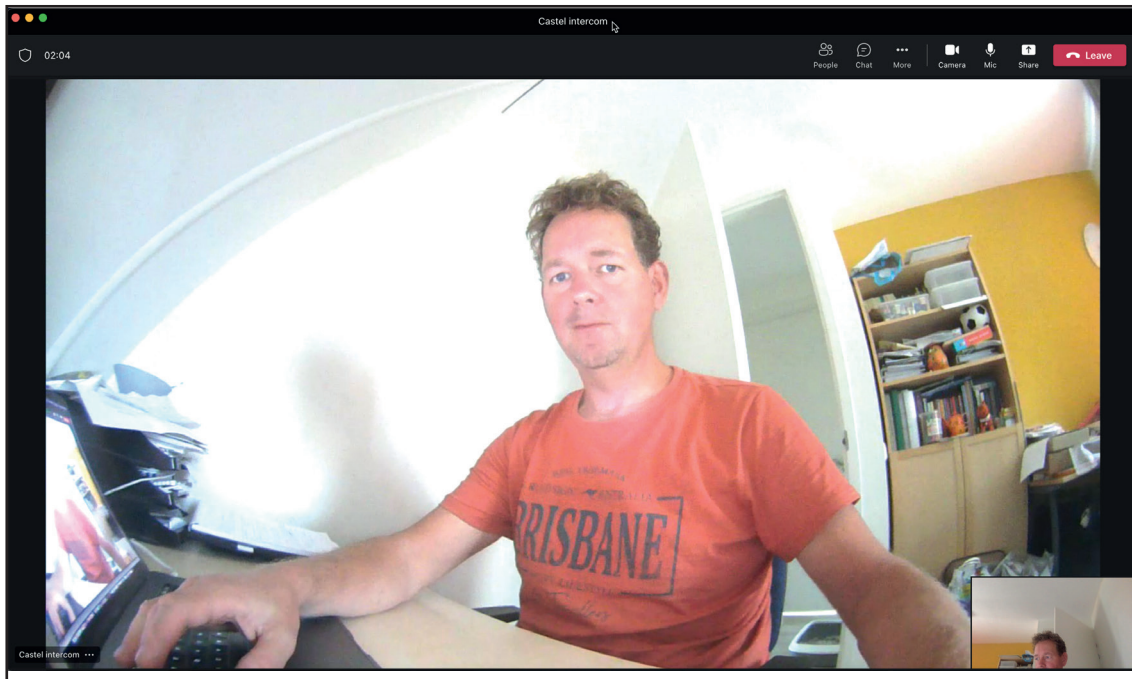
Click the blue 'Save' button when done.



Configuration of the Castel is now finished.
Pressing the call button on the Castel will initiate a call to the number that is configured in the Function key menu.



The call will be established and video will be displayed within ± 3 seconds.



To open the door from the Teams call, click on the three dots (...) in the call screen and select the 'Keypad'.

Use the '0' code, this will trigger the relay in the Castel and open the door.

APPENDIX - Install the CyberGate App

Requirements for the CyberGate app

Requirements for using the CyberGate App:

1. A subscription to one of the following CyberGate SaaS solutions:
 - CyberGate for IP Cameras with Teams
 - CyberGate for IP Paging with Teams
 - CyberGate for IP Intercoms with Teams
2. Access to the Microsoft Teams admin portal

Introduction

The CyberGate Teams app is an app that can be installed in your Microsoft Teams client. It is developed to offer extra functionality using CyberGate.

The CyberGate app has three main features:

1. When using CyberGate Multi-ring groups, the app allows you to set availability status in a Multi-ring group
2. It offers a Devices overview page. This page shows the current status of the device (online or offline) and features a Connect-button. Using this button you can initiate a call from Teams to the device with just one click
3. Easily open the door during a Teams call with an intercom device by clicking a Door open button

This manual will describe the installation of the app and all three features in detail.

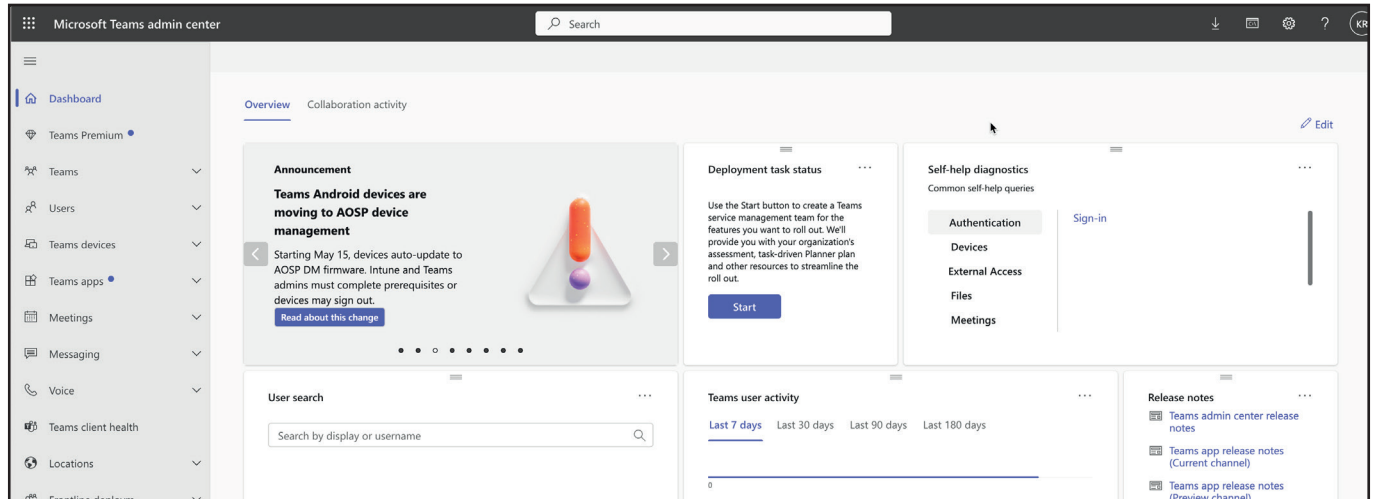
The installation of the CyberGate app for Microsoft Teams as described in this document makes the CyberGate app available for every user in the organisation. Of course this can be modified by selecting different user groups and / or setup policies to match the policies of your organisation.



Installation

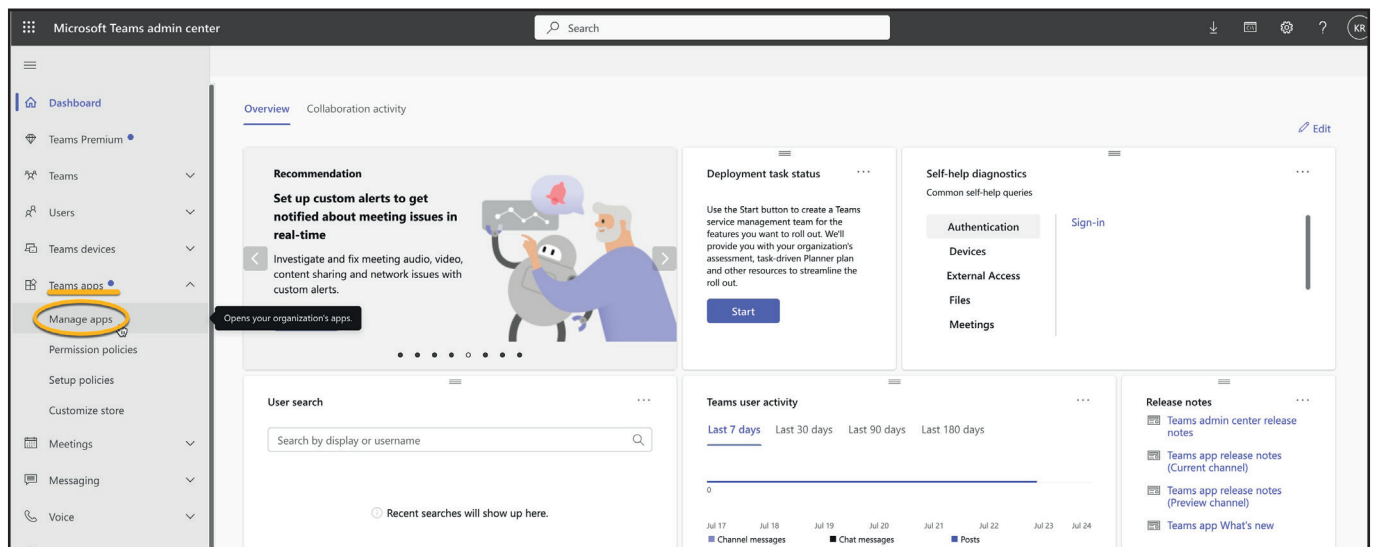
How to install

- Log in to the Microsoft Teams Admin Portal (<https://admin.teams.microsoft.com>)



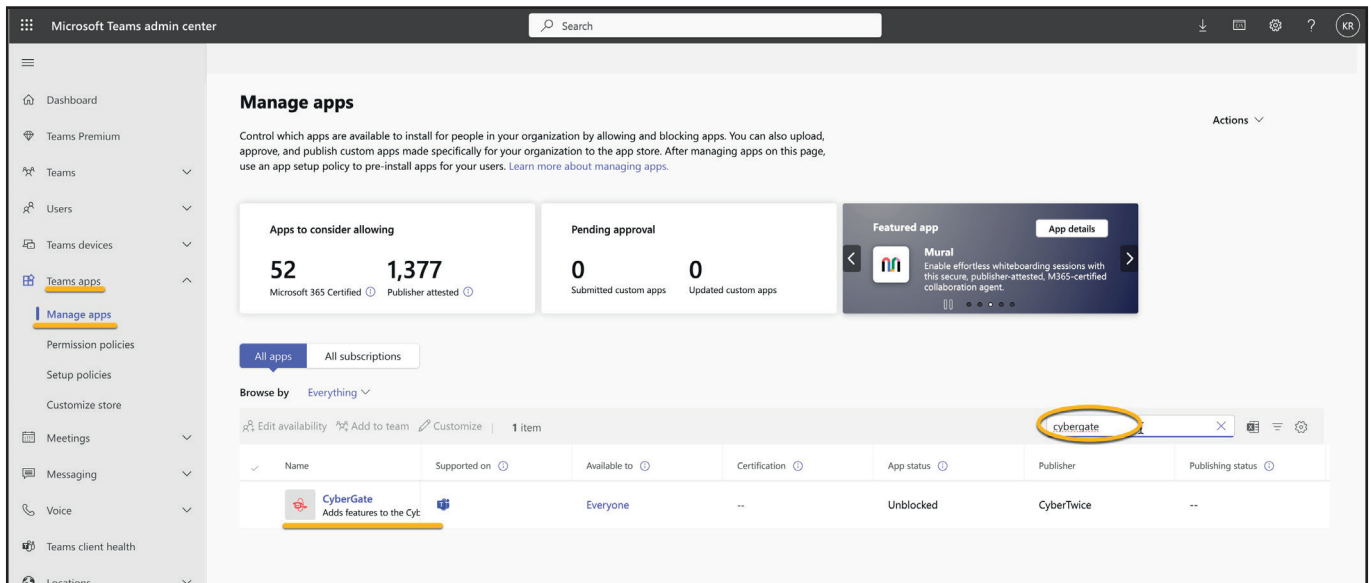
Microsoft Teams Admin Portal - Dashboard

- Navigate to the menu Teams apps - Manage apps



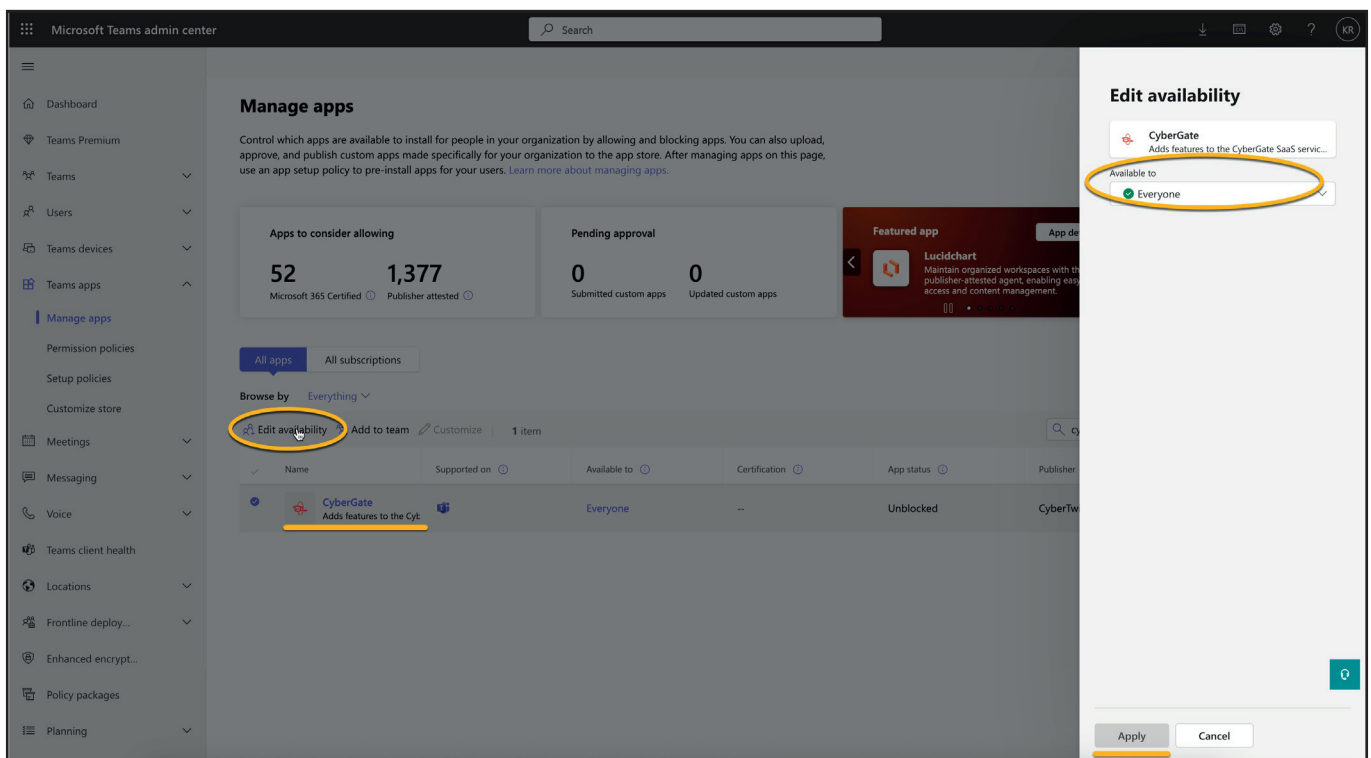
Microsoft Teams Admin Portal - Teams apps - Manage apps

- Search for 'CyberGate' using the search box. The CyberGate application will show.



Microsoft Teams Admin Portal - Teams apps - Manage apps - Search for CyberGate

- Select the found 'CyberGate' and click on 'Edit availability'. Set the CyberGate availability to 'Everyone' and click 'Apply'.



Microsoft Teams Admin Portal - Teams apps - Set availability to 'Everyone'

- Navigate to the menu Teams apps - Setup policies

The screenshot shows the Microsoft Teams Admin Center interface. The left-hand navigation menu is visible, with 'Setup policies' highlighted and circled in orange. The main content area displays the 'App setup policies' page, which includes a summary card showing 2 Default policies and 0 Custom policies. Below the summary, there are buttons for 'Manage policies' and 'Group policy assignment'. A table lists the existing policies:

Name	Description	Custom policy
Global (Org-wide default)		No
FirstLineWorker	This is a default app set...	No

Microsoft Teams Admin Portal - Teams apps - Setup policies

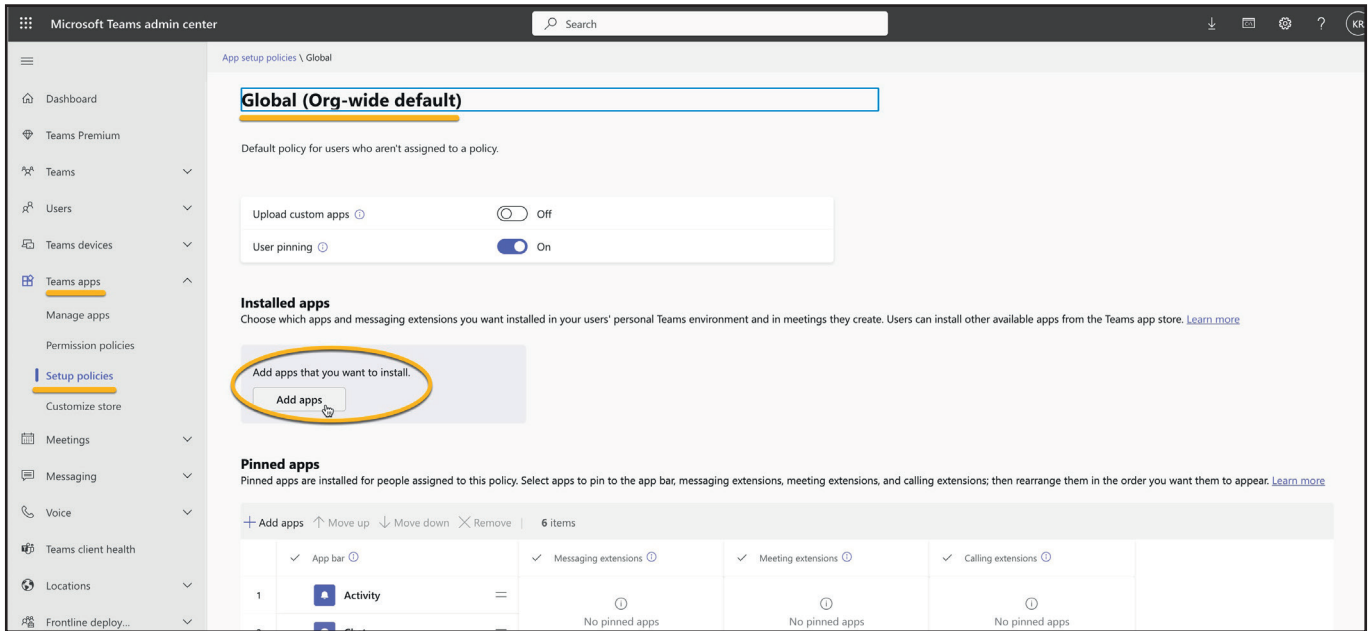
- Select the policy 'Global (Org-wide default)'

The screenshot shows the Microsoft Teams Admin Center interface, similar to the previous one. In this view, the 'Global (Org-wide default)' policy in the table is circled in orange. The table content is as follows:

Name	Description	Custom policy
Global (Org-wide default)		No
FirstLineWorker	This is a default app set...	No

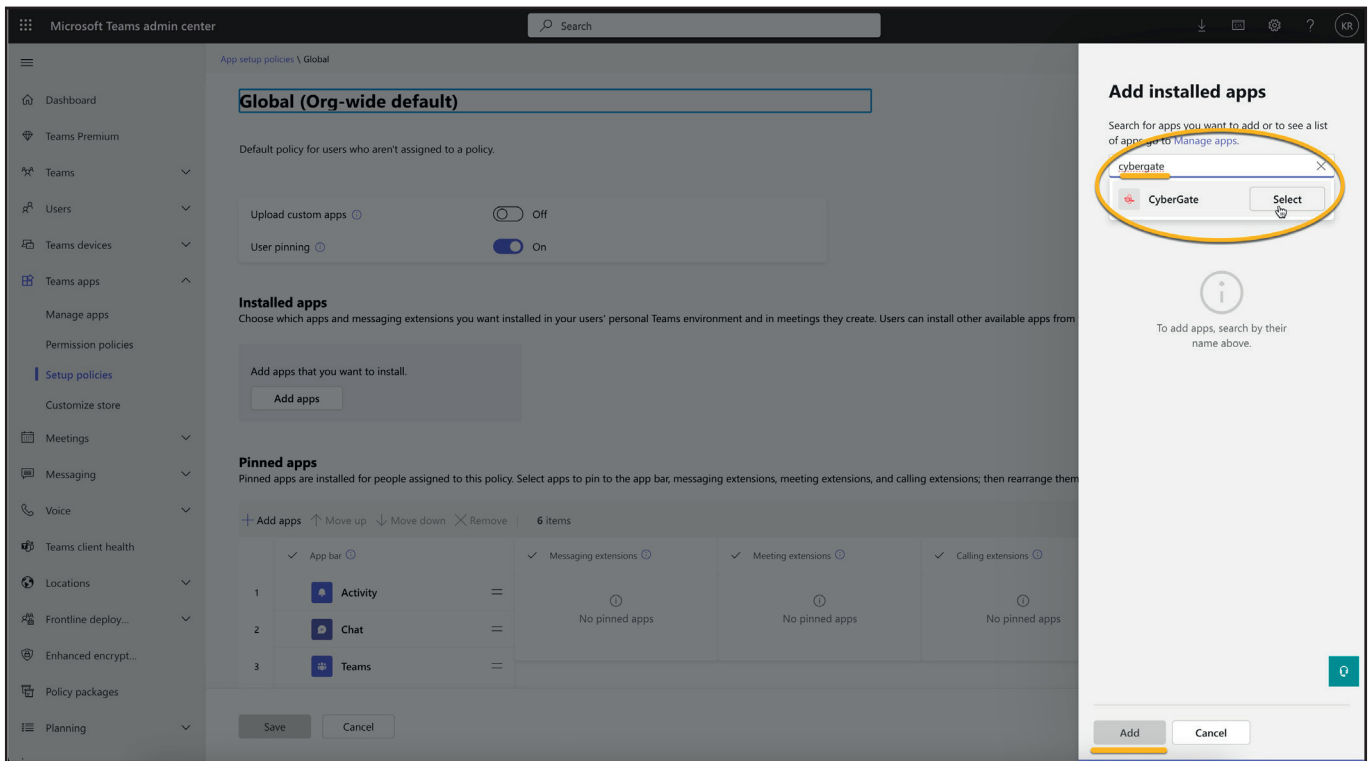
Microsoft Teams Admin Portal - Teams apps - Setup policies - Select 'Global'

- At 'Installed apps', click Add apps to add CyberGate



Microsoft Teams Admin Portal - Teams apps - Setup policies - Add apps

- Search for CyberGate in the search box, select it and add CyberGate.



Microsoft Teams Admin Portal - Teams apps - Setup policies - Installed - Search and select CyberGate

The CyberGate app will show as installed.

The screenshot shows the Microsoft Teams Admin Center interface. The left sidebar contains navigation options like Dashboard, Teams Premium, Users, Teams devices, Teams apps, Meetings, Messaging, Voice, Teams client health, Locations, Frontline deploy..., and Enhanced encrypt... The main content area is titled 'App setup policies \ Global' and shows the 'Global (Org-wide default)' policy. Under 'Installed apps', a table lists the 'CyberGate' app with App ID '8dd84f10-2fbf-4c8b-9116-7eb326bd7c8e' and Publisher 'CyberTwice'. The 'Pinned apps' section shows a table with columns for App bar, Messaging extensions, Meeting extensions, and Calling extensions, all currently empty.

Microsoft Teams Admin Portal - Teams apps - Setup policies - CyberGate added to the organisation

- At Pinned apps, click 'Add apps' to add CyberGate to the Teams environment of the users.

This screenshot shows the 'Pinned apps' section of the Microsoft Teams Admin Center. The 'Add apps' button is circled in red. The table below shows the current pinned apps: Activity, Chat, Teams, Calendar, Calling, and OneDrive. The 'Add apps' button is located at the top left of the pinned apps table.

Microsoft Teams Admin Portal - Teams apps - Setup policies - Add CyberGate to the Pinned apps

- Search for CyberGate in the search box, select it and add CyberGate

The screenshot displays the Microsoft Teams Admin Portal interface. The main content area is titled "Add pinned apps" and includes a search box with the text "cybergate" entered. Below the search box, a list of search results shows "CyberGate" with a "Select" button next to it. The "Add" button at the bottom of the panel is highlighted in yellow. The background shows the "Pinned apps" section of the Teams admin center, which lists several apps like Activity, Chat, Teams, Calendar, Calling, and OneDrive.

Microsoft Teams Admin Portal - Teams apps - Setup policies - Pinned - Search and select CyberGate

The CyberGate app will show as pinned in the App bar and in the 'Calling extensions'.

The screenshot displays the Microsoft Teams Admin Center interface. The left-hand navigation pane is open to 'Setup policies' > 'Customize store'. The main content area shows the 'Global (Org-wide default)' policy configuration. Under 'Installed apps', the 'CyberGate' app is listed with App ID '8dd84f10-2bf-4c8b-9116-7eb326bd7c8e' and Publisher 'CyberTwice'. Under 'Pinned apps', the 'CyberGate' app is pinned to the 'App bar' and 'Calling extensions' sections. The 'App bar' section shows 'CyberGate' as the first pinned app, followed by 'Activity', 'Walkie Talkie', 'Chat', 'Teams', 'Calling', 'Calendar', and 'OneDrive'. The 'Calling extensions' section shows 'CyberGate' as the only pinned extension. The 'Messaging extensions' and 'Meeting extensions' sections are currently empty.

Microsoft Teams Admin Portal - Teams apps - Setup policies - CyberGate successfully pinned

The policy change will take up to 24 hours. After that, the CyberGate app will be available for the Teams users in the organisation..

Availability

How to use

The CyberGate app uses the same credentials as used for Microsoft Teams. It automatically retrieves information from CyberGate regarding the Multi-ring groups the user is part of.

In this example, the user `koos.ridder@cybertwice.com` is part of two Multi-ring groups:

- Sales personnel group
- The wall group

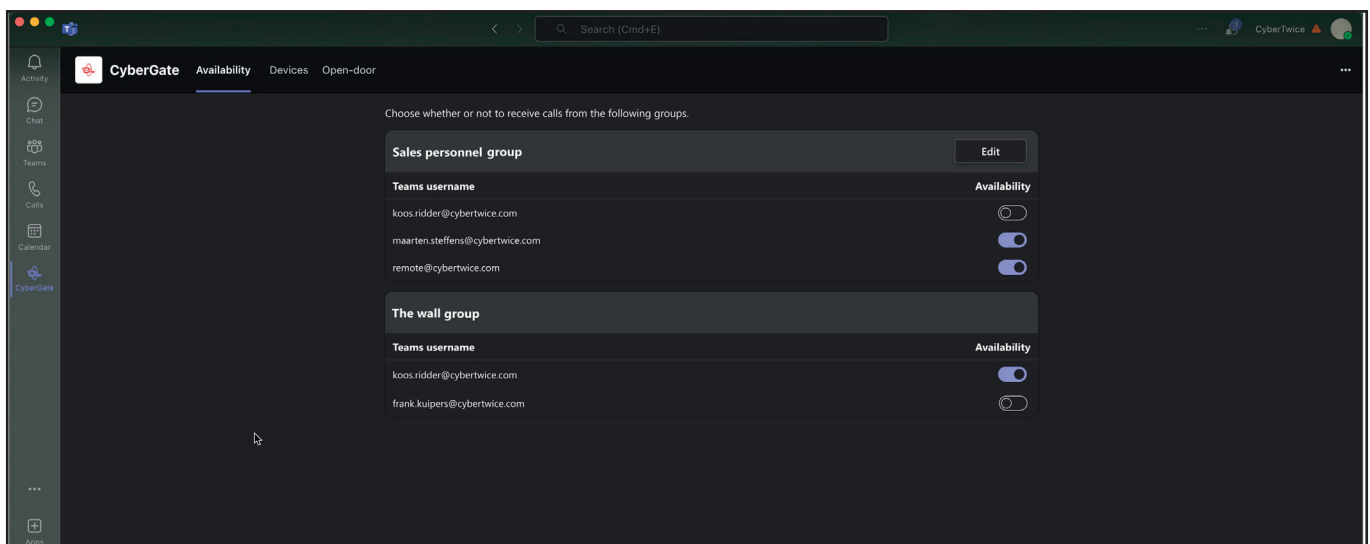
The 'Sale personnel group' contains three users and the 'The wall group' contains two users.

In the 'Sale personnel group', the user `koos.ridder@cybertwice.com` is supervisor (*) and can therefore set the availability status of all users in this Multi-ring group. He can also edit this Multi-ring group (add / remove users).

In the 'The wall group', the user `koos.ridder@cybertwice.com` is a normal user and can only set his own availability status.

The availability status takes effect immediately.

- Available: You are available in the Multi-ring group and therefore you can be called by CyberGate
- Unavailable: You are not available in the Multi-ring group and won't be called by CyberGate



CyberGate App - Availability

Note:

To configure the supervisor role for a Multi-ring group, use the CyberGate Management Portal (admin.cybergate.cybertwice.com).

Devices

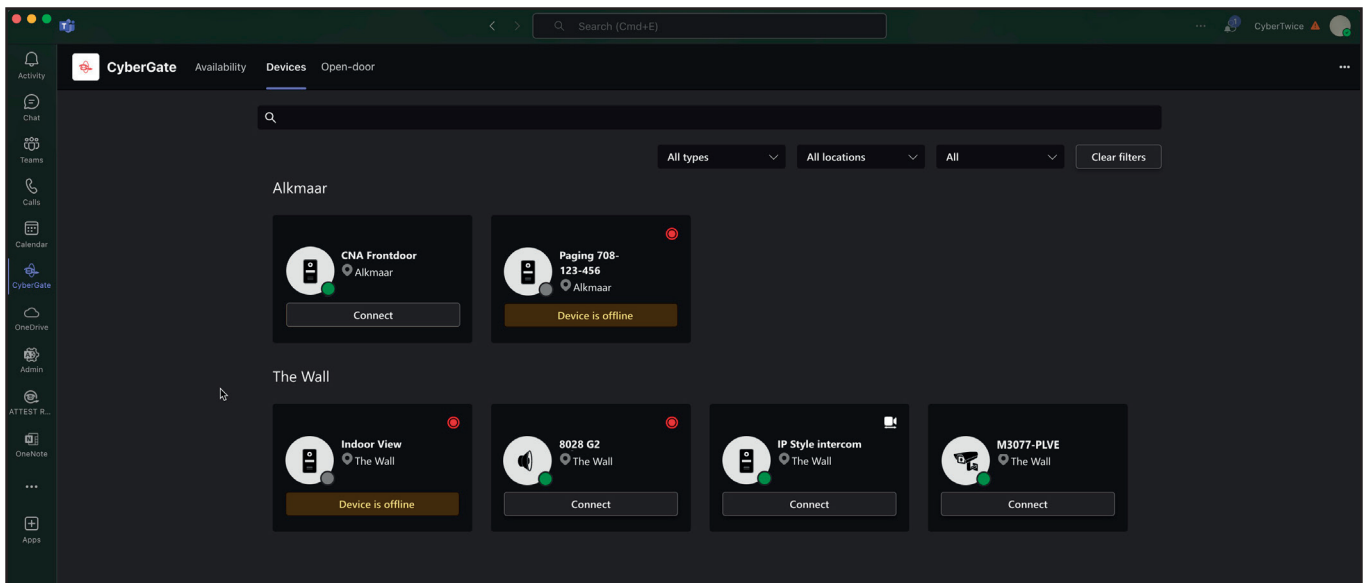
How to use

The Devices menu provides an overview of the configured devices in your Tenant. The view is sorted by location of the devices and the results can be filtered to search a specific device.

Each device is shown as a tile. The tile shows the following information:

- The device type - intercom, camera or audio / paging
- The device name
- The online status - is a device online or offline
- Recording status - is recording enabled for this device
- Two way video - is two-way video configured for this device

A Connect button is available if a device is configured to be called to from Microsoft Teams. Clicking on this button initiates a call to this device.



CyberGate App Devices Tab - Configured CyberGate devices

Note:

The devices shown to a user in the Devices menu can be limited using the Device access settings in the CyberGate Management Portal (admin.cybergate.cybertwice.com).

Door-open button

Introduction

The CyberGate app also features a so called 'Door-open button'. During a call between the intercom and a Teams user you can easily open the door by clicking on a button on the sidebar.

How to activate

Follow the next steps to activate the Door-open button.

- Log in to the CyberGate management portal and navigate to the Basic-Device menu.

CyberTwice Koos Ridder
fr in.onmicrosoft.com

ADMINISTRATION

- Licensing

BASIC

- Global
- Network
- Portal access
- Device
- Multi-ring

CAMERA

- Meeting

TEAMS APP

- Availability
- Device

Device settings

Create a device entry for each SIP device you are connecting to CyberGate.
Each created device entry contains an authentication username and password to be used in the configuration of your SIP device together with 'cybergate.cybertwice.com' as the registrar address.
For detailed instructions on how to configure the SIP device click [here](#) for the brand specific manuals.

To make the display name visible and to enable video in Teams, some configuration in the Teams environment is required.
This can be done automatically by executing the PowerShell script that can be downloaded with the button below.
The user to execute this script must have either the Global Administrator role or both the User Administrator role and the Teams Administrator role.
For more information see the [manual](#).

[Download](#)

[Add device](#)

Display name	Authentication username	Password	Licensed	Recorded	Teams to device	Action
Test location						
Test device	QV9ZTCASCUSHH0A5CHFA	AZZ ●●●●●●●●	yes	no	yes	Edit Delete

CyberGate Management Portal - One configured device

- Click on the blue edit button to open the device details and fill in the 'Open door code'.
- Click on the blue Update button when done.

Note:

The 'Open door code' must match the configured open door code in the intercom device!

Update Device [Close]

Display name
Intercom Frontdoor
This name is used as a display name within Teams

Type
Intercom [v]
The device type is used for administrative use only

Location
Amsterdam
The device location is used for administrative use only

Record device

Allow 2-way video ⓘ

For compatible devices that support receiving video.

Allow calls from Teams to device

For devices that support incoming SIP calls.

Open door code (optional)

The open door code is sent as DTMF to the device when the open door button in the CyberGate for Microsoft Teams App is pressed. Only DTMF characters are allowed (0123456789 *#).

Detected SIP username
MONET

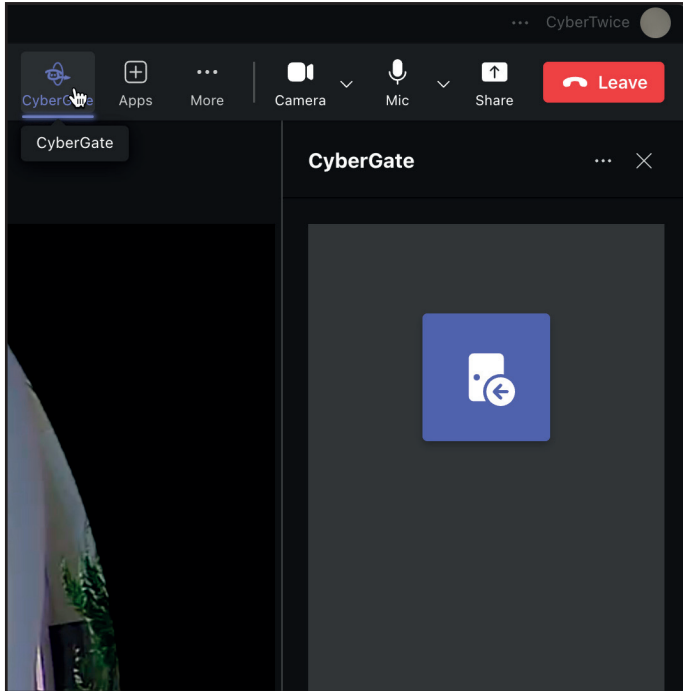
[Cancel] [Update]

CyberGate Management Portal - Device details

A

During a call from the intercom, click on the CyberGate logo in the top bar. A sidepanel will open revealing the Open door button.

- Click the button to open the door.



CyberGate Management Portal - Open door button

- End the call.

The Open door button is available automatically during intercom calls.

Document History

Document Version	Date	Author	Change
1.0.0	29-07-2022	KR	Initial version
1.0.1	23-02-2024	KR	Fixed codec selection
1.0.2	05-11-2024	KR	Updated layout
1.0.3	07-11-2024	KR	Fixed text and added “CyberGate app” appendix
1.0.4	14-08-2025	KR	Modified “CyberGate app” appendix