



## TechNote: AXIS and CyberGate

## AXIS OS 11

Version: 1.0.6 ENG  
Date: 13-08-2025



Configure the AXIS Network Video Door  
Station for the CyberGate service

## 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 an AXIS Network Video Door Station to your Microsoft Teams environment. Microsoft Teams users can answer incoming calls from- or place outgoing calls to the intercom – 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.

*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'.*



# A

## AXIS Network Video Doorstation

For this document the AXIS A8207-VE MK II Network Video Doorstation (from now on named 'AXIS') is used to connect to the CyberGate service (from now on named 'CyberGate').

This manual also applies to the following Axis Video Doorstations running AXIS OS 11:

- AXIS I8116-E
- AXIS I7010-VE
- AXIS I8016-LVE

Follow the next steps to configure the AXIS 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 AXIS

Login as 'root' with the configured password

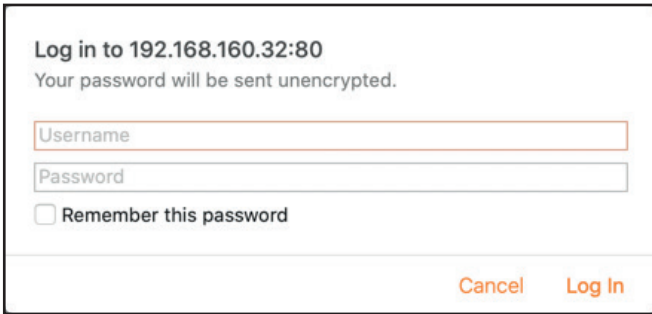


Fig.1: AXIS - Log in

When logged-in, the live view opens

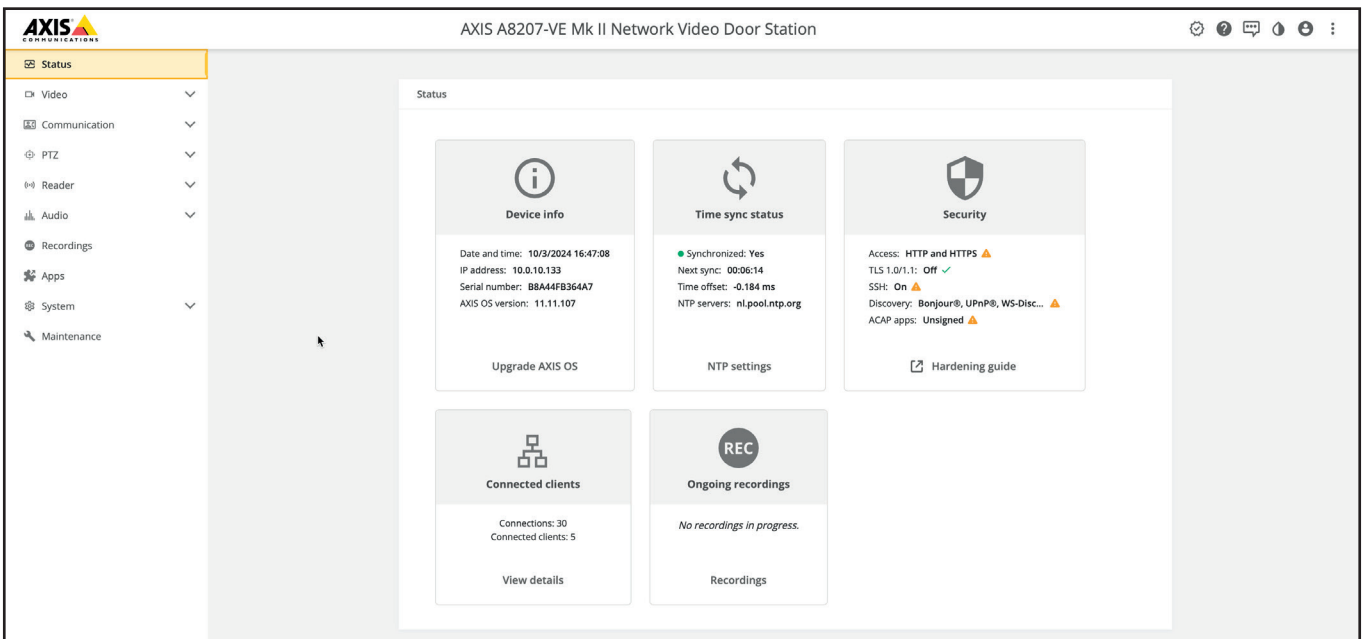


Fig.2: AXIS - Status

Navigate the -Communication-SIP- menu, select 'Start new configuration' and click 'Start'.

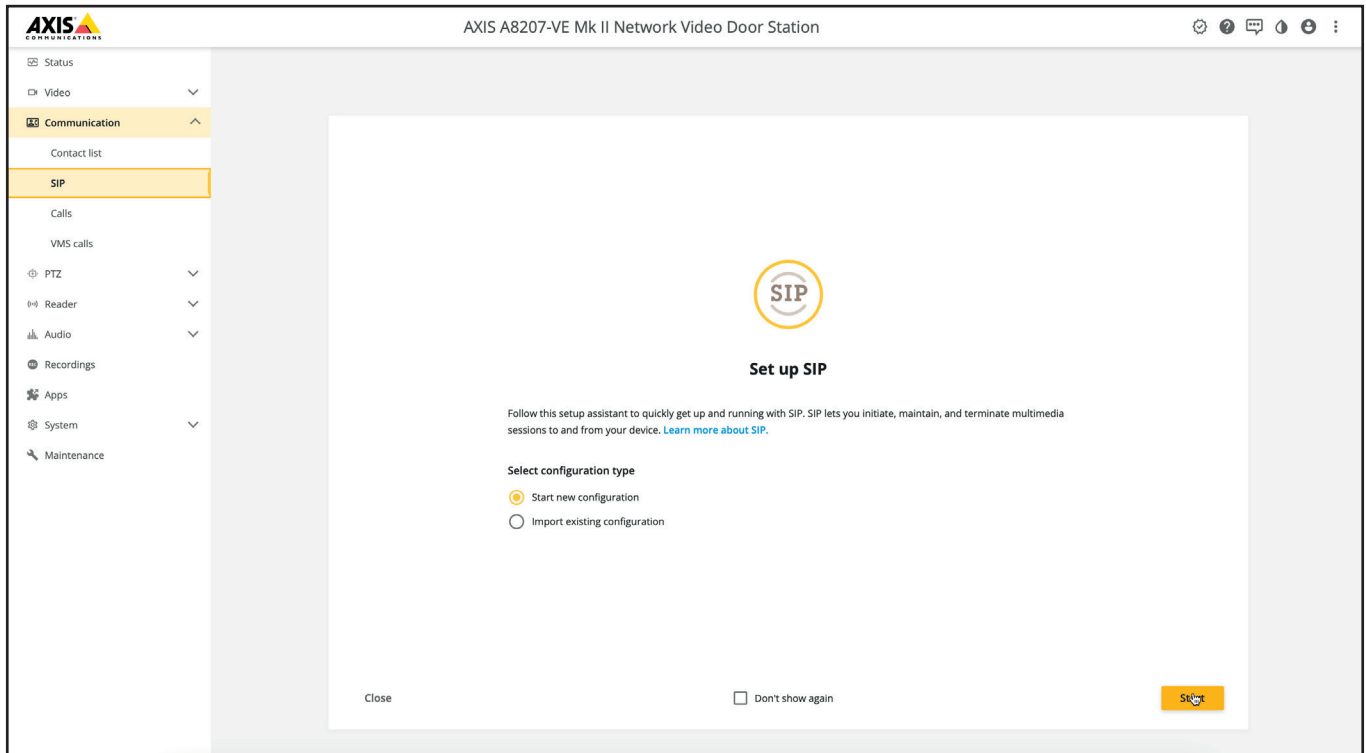


Fig.3: AXIS - Setup SIP

Enable SIP and allow incoming SIP calls and click 'Next'.

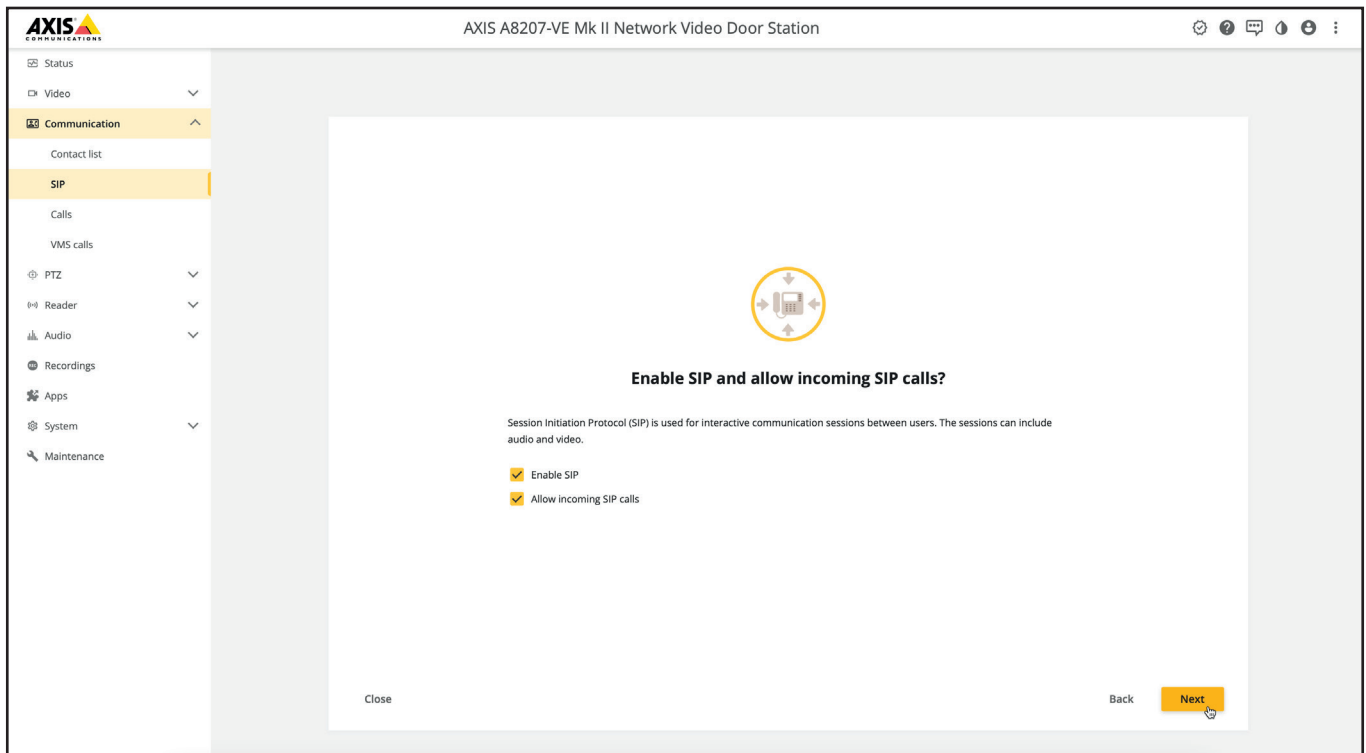


Fig.4: AXIS - Enable SIP

Select the Registered Account type and click 'Next'.

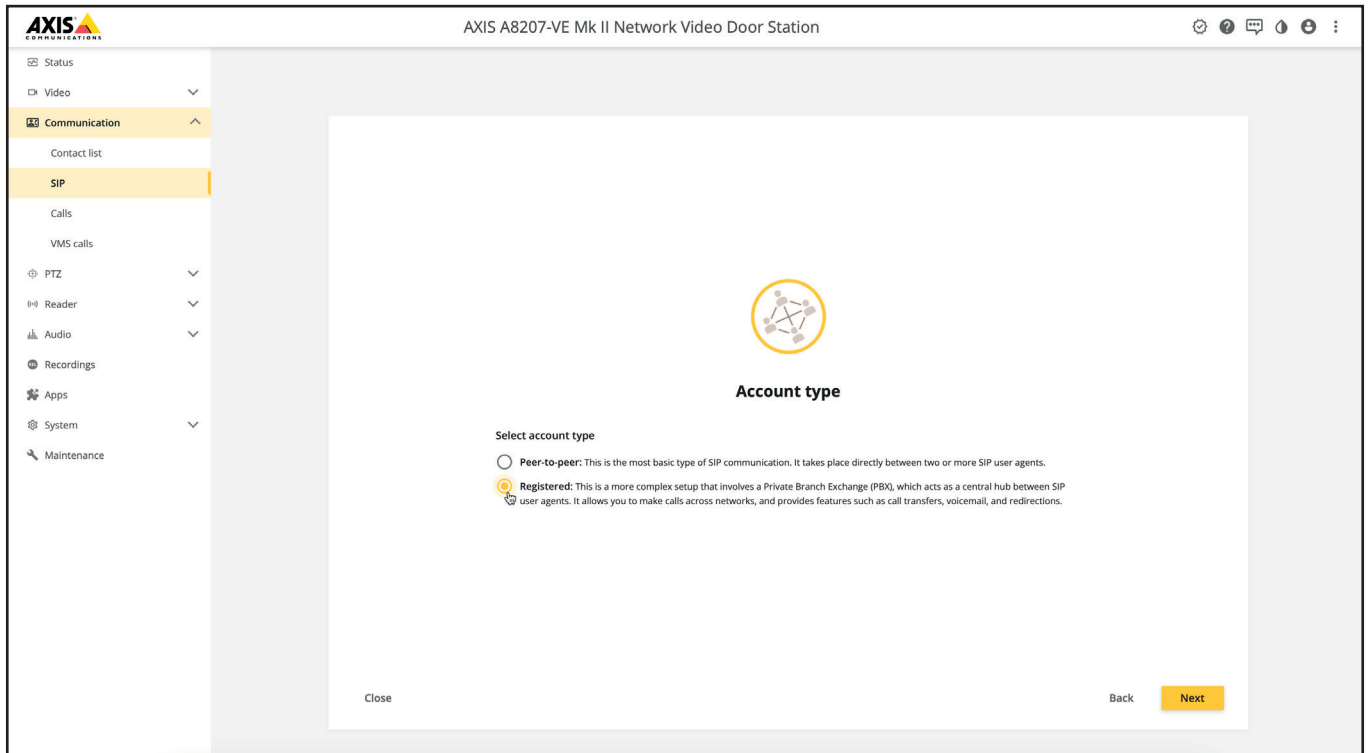


Fig.5: AXIS - Account type

Create a registered account by filling in the following information:

Name	Name of the SIP account, in this example 'CyberGate'
User ID	Use the Username provided by the CyberGate service
Domain	Use the domain name of your organisation
Password	Use the Password provided by the CyberGate service

Click 'Next'.

The screenshot shows the configuration interface for the AXIS A8207-VE Mk II Network Video Door Station. The left sidebar contains a navigation menu with options: Status, Video, Communication (expanded), Contact list, SIP (selected), Calls, VMS calls, PTZ, Reader, Audio, Recordings, Apps, System, and Maintenance. The main content area displays a progress bar for the 'Registered' process, with steps: New, SIP, Account type, Account (current step), DTMF, Contact, Apply settings, Test call, and Export. Below the progress bar, the 'Create a registered account' form is visible, containing the following fields and instructions:

- Name \***: Enter a descriptive name for the account. The name is not unique. (Value: CyberGate)
- User ID \***: Enter the unique extension or phone number assigned to the device. (Value: 5LLBA72V5X7JRPDJZEPV)
- Domain \***: Enter the PBX server address or public domain name. (Value: cybergate.cybertwice.com)
- Password**: Enter the password associated with the user ID for authenticating against the PBX server. (Value: masked with dots)

At the bottom of the form, there are 'Close', 'Back', and 'Next' buttons.

Fig.6: AXIS - Create account

Configure DTMF by filling in the following information:

DTMF Description	Name the Action that is triggered by DTMF
Sequence	Enter the character that is used to open the door
Rule name	Name the open-door rule

Click 'Next'.

The screenshot shows the configuration interface for the AXIS A8207-VE Mk II Network Video Door Station. The left sidebar contains a navigation menu with options like Status, Video, Communication, Contact list, SIP, Calls, VMS calls, PTZ, Reader, Audio, Recordings, Apps, System, and Maintenance. The main content area is titled 'Configure DTMF' and includes a progress bar with steps: New, SIP, Account type, Account, DTMF (current), Contact, Apply settings, Test call, and Export. The 'Configure DTMF' section contains the following text and form fields:

**Registered**

Use DTMF to send commands in SIP calls. The DTMF character range consists of digits 0-9, letters A-D, \* and #. For example, in a SIP call, the user sends the character '5' from the phone's keypad, which has been configured to unlock the door on the receiver side.

Set up DTMF and create a DTMF rule in the device's event system. If you want to add more rules when the setup is done, go to System > Events.

**DTMF description \***  
Enter a description of the action that you want the DTMF sequence to trigger.  
DTMF to unlock the door

**Sequence \***  
Enter the characters that will activate the rule.  
5

**Rule name**  
Enter a name for the rule you want to create in the device's event system.  
OpenDoor

**Port**  
Select which port will be used when the action triggers.  
Door

**State**  
Select the state in which the action should trigger.  
Active

At the bottom of the form, there are three buttons: 'Close', 'Skip', and 'Next'.

Fig.7: AXIS - Configure DTMF

Create the contact to call when the button is pressed by filling in the following information:

First name	The first name of the contact
Last name	The last name of the contact
SIP address	Use the Teams user name followed by the domain 'cybergate.cybertwice.com' <name.name>@cybergate.cybertwice.com *

\* For example, the user 'Koos Ridder, with the Teams name:

*koos.ridder@mycompany.com*

will translate to this destination address:

*koos.ridder@cybergate.cybertwice.com*

Click 'Next'.

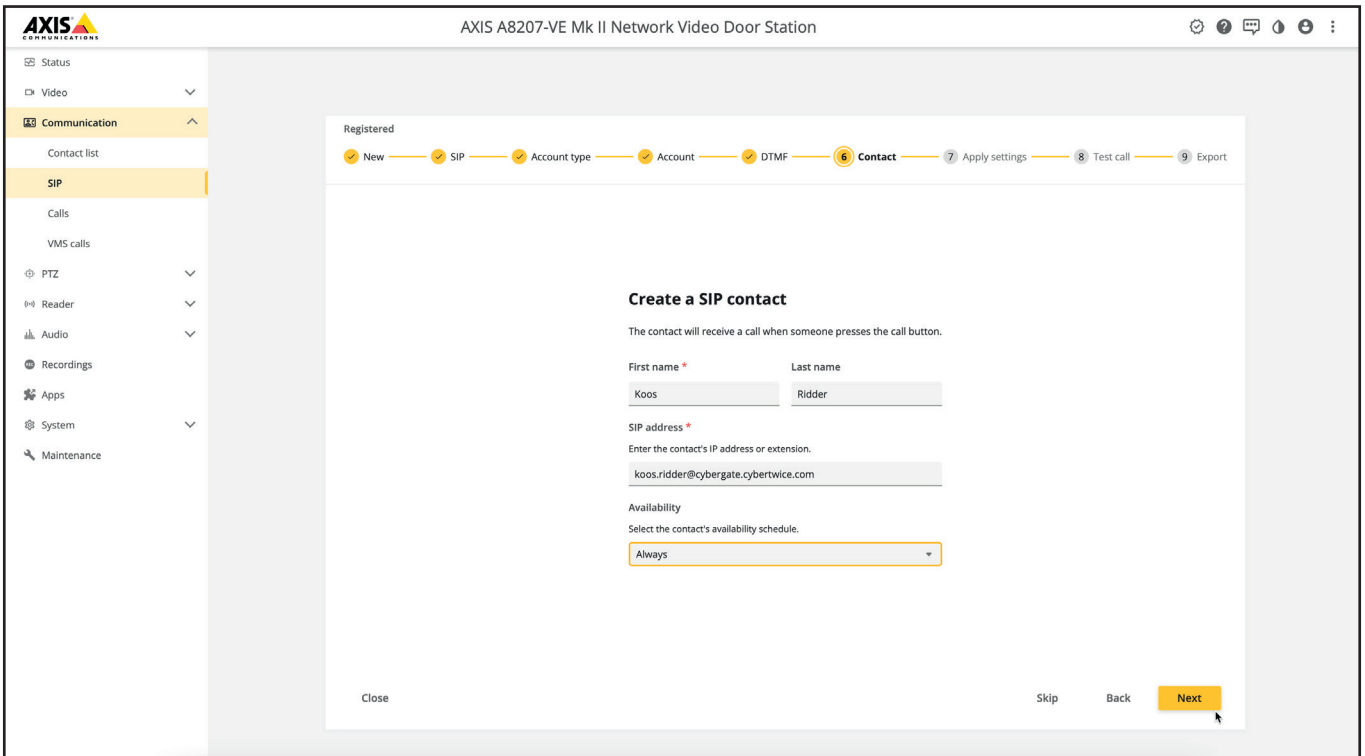


Fig.8: AXIS - Create contact

Test your setup with the yellow phone symbol. If it rings the Teams user and has audio and video, click 'Next'.

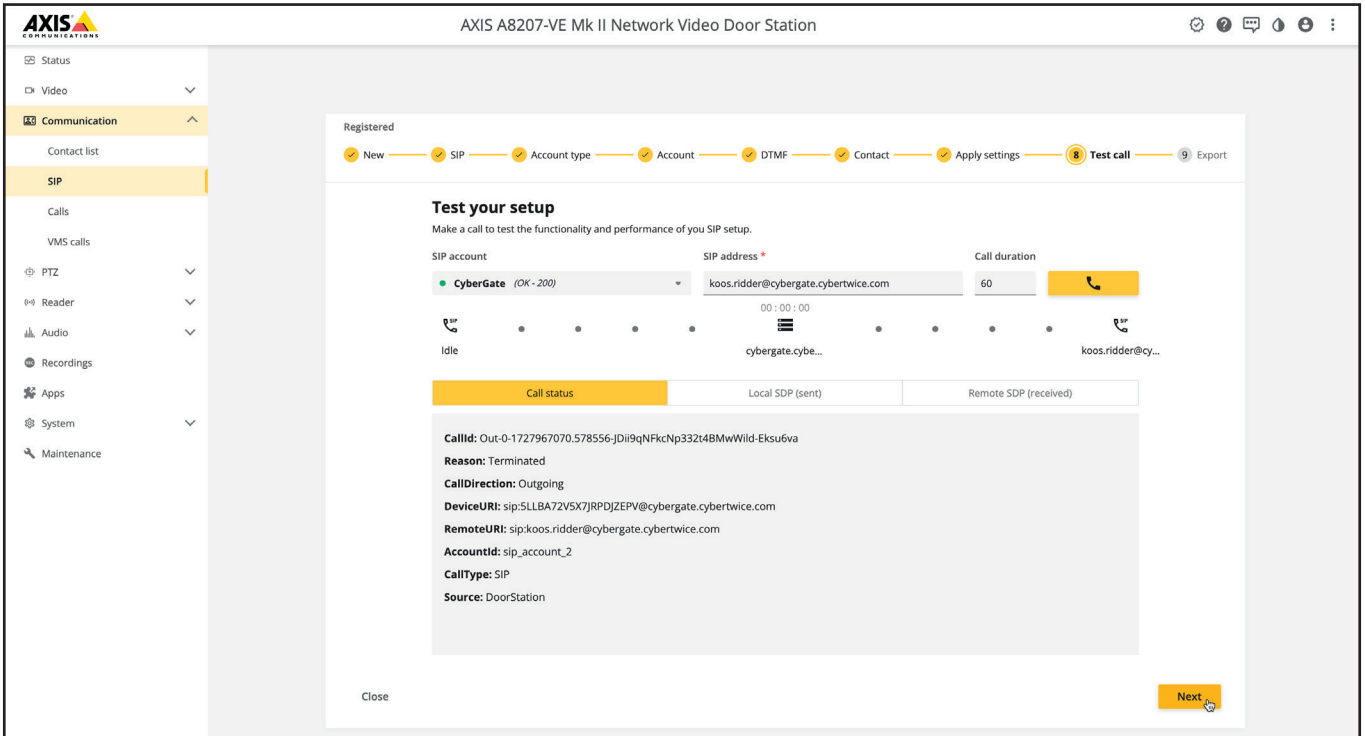


Fig.9: AXIS - Test setup

Setting up the AXIS is done.

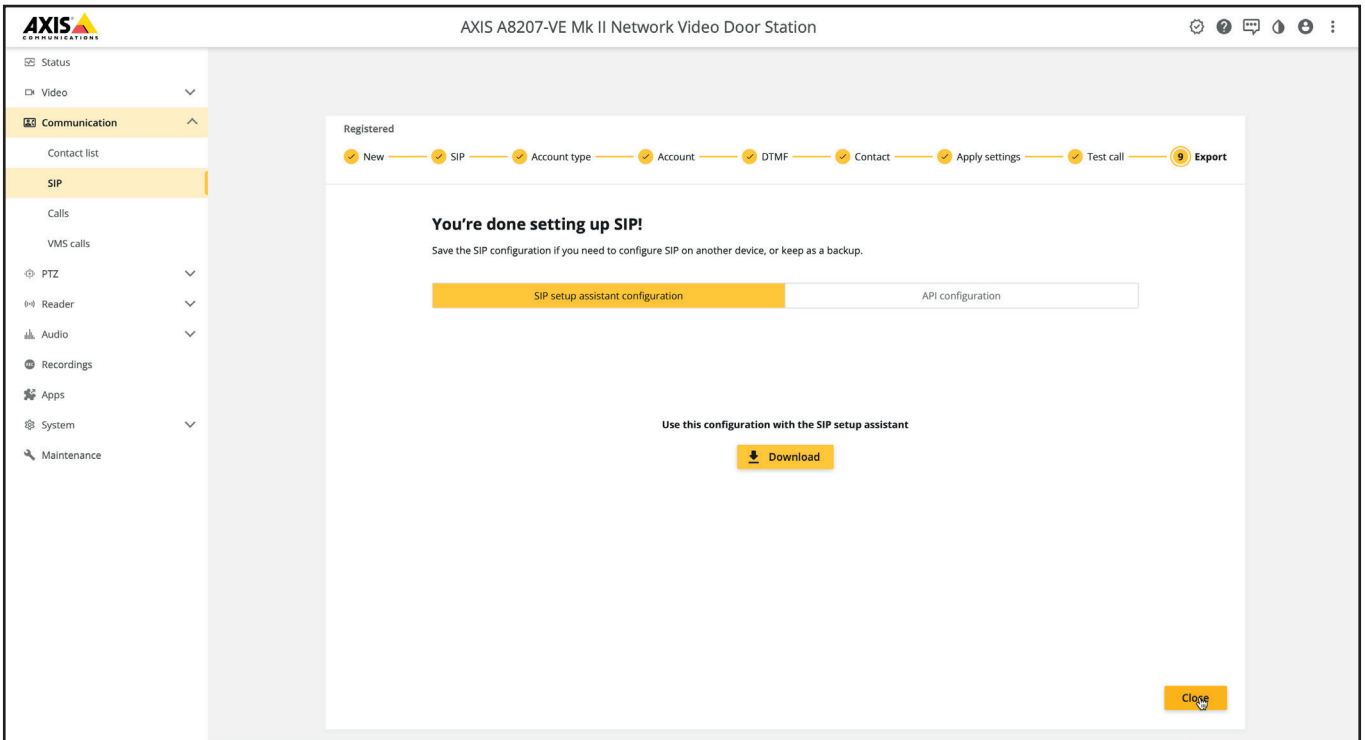


Fig.10: AXIS - Setup done

## Secure connection to CyberGate

By default the AXIS uses TCP to connect to CyberGate. If you need the communication to be secure it will need to use SIP TLS.

To connect to CyberGate securely via SIP TLS, navigate to the menu -Communication-SIP- and close the setup assistant.

Navigate to 'Accounts' and click on the three vertical dots at the end of your SIP account.

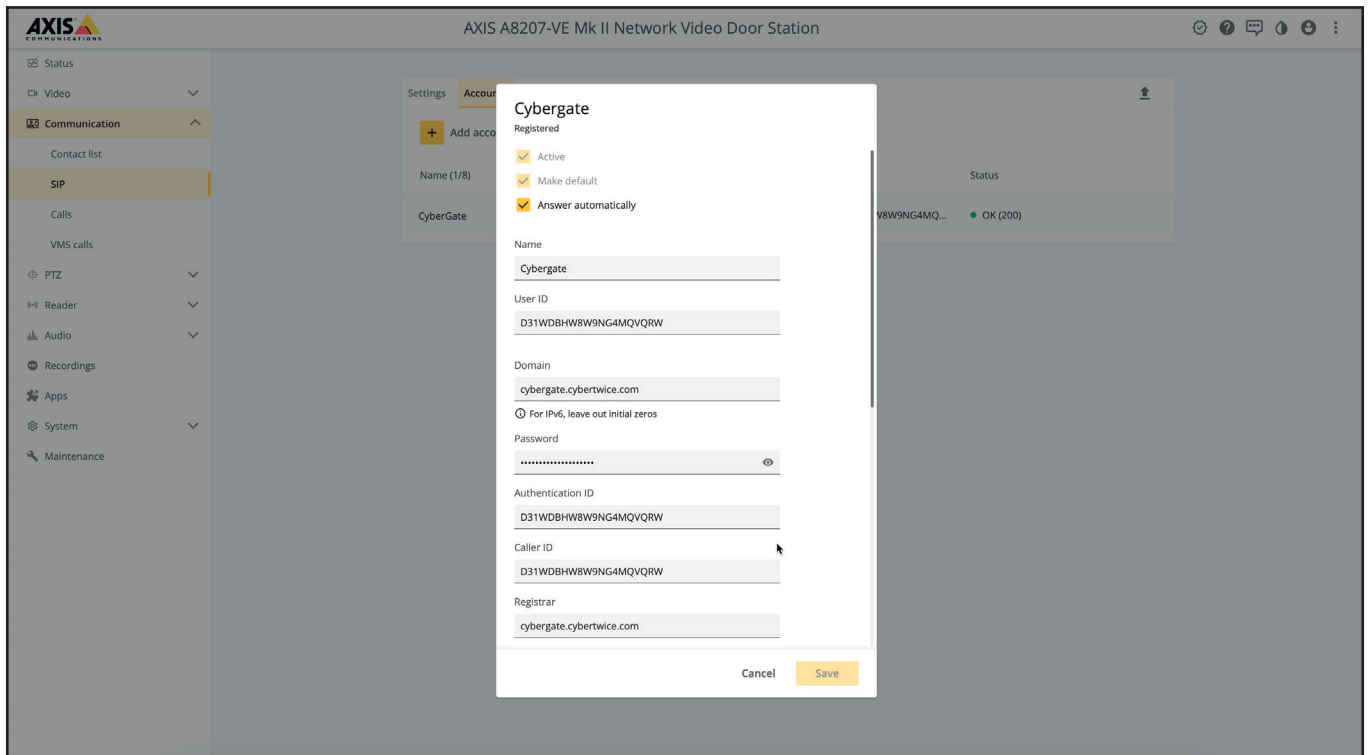


Fig.11: AXIS - Edit account

Scroll down and modify the following information:

Transport Mode	Change to TLS
TLS version	Select v1.2
Media Encryption	Change to SRTP Mandatory
Client certificate	Change to Default (self-assigned)

Click the Save button to confirm.

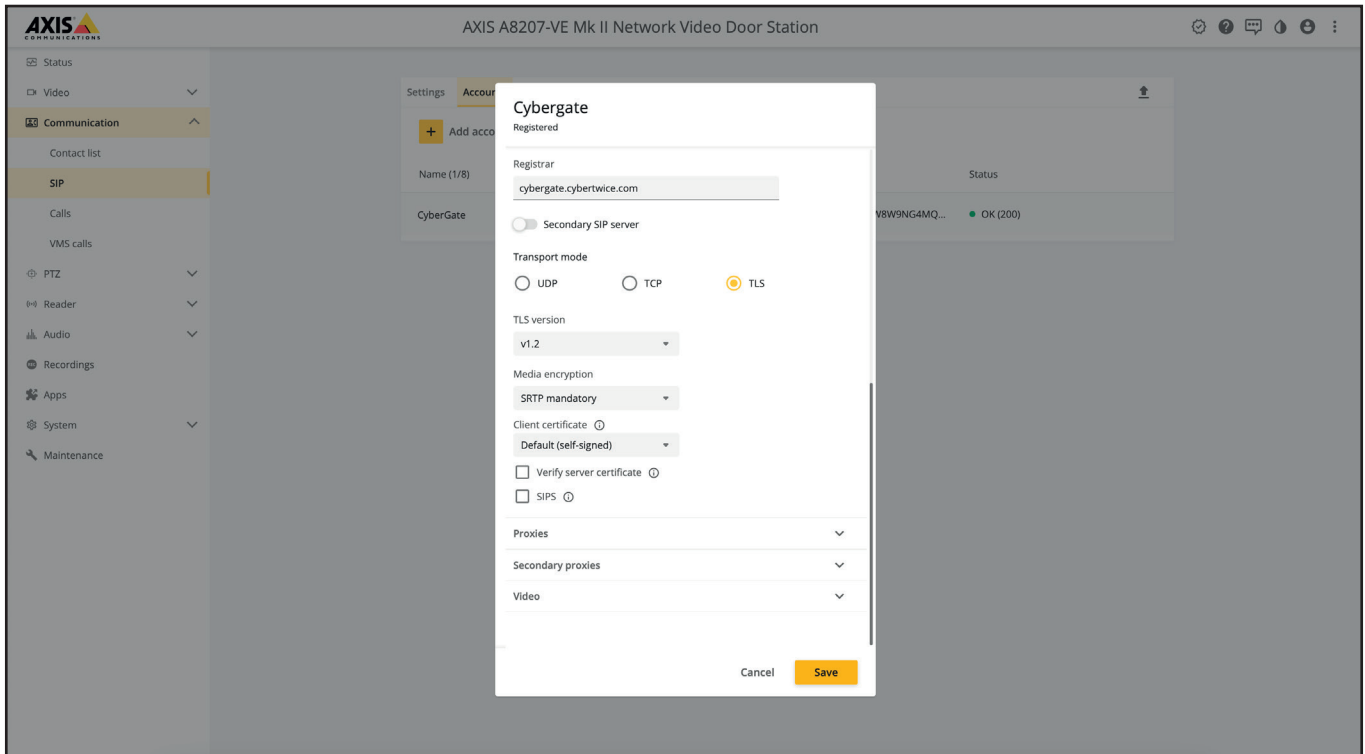


Fig.12: AXIS - Set to TLS

These settings ensure that the SIP traffic and the audio / video are encrypted.

After configuration, press the button on the AXIS to call the Teams recipient. If configured correctly, the Teams client will notify you of an incoming call. Answer it by clicking the answer button.

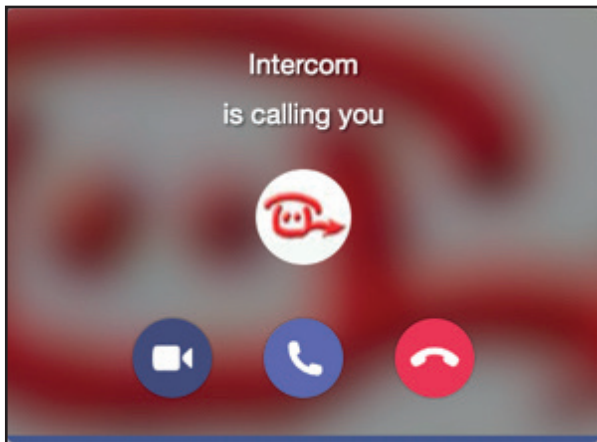


Fig.13: Incoming call in Teams

The call will be established and video will be displayed within  $\pm 3$  seconds.

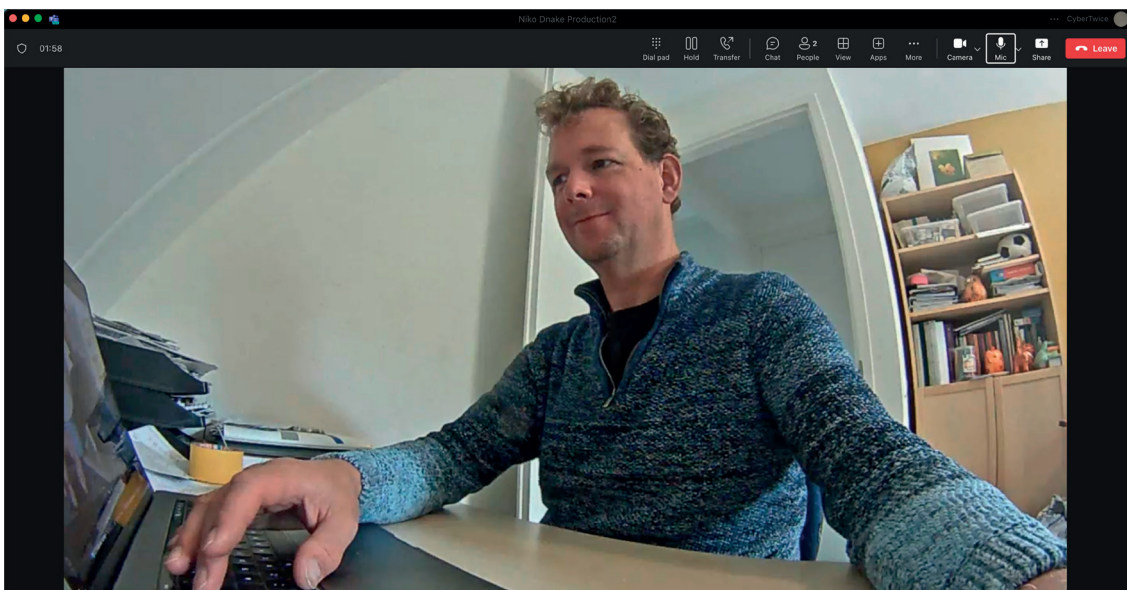


Fig.14: Live video

To open the door from the Teams call, click 'Dial pad' on top of the active call screen. Use the DTMF code (as configured before) to 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.

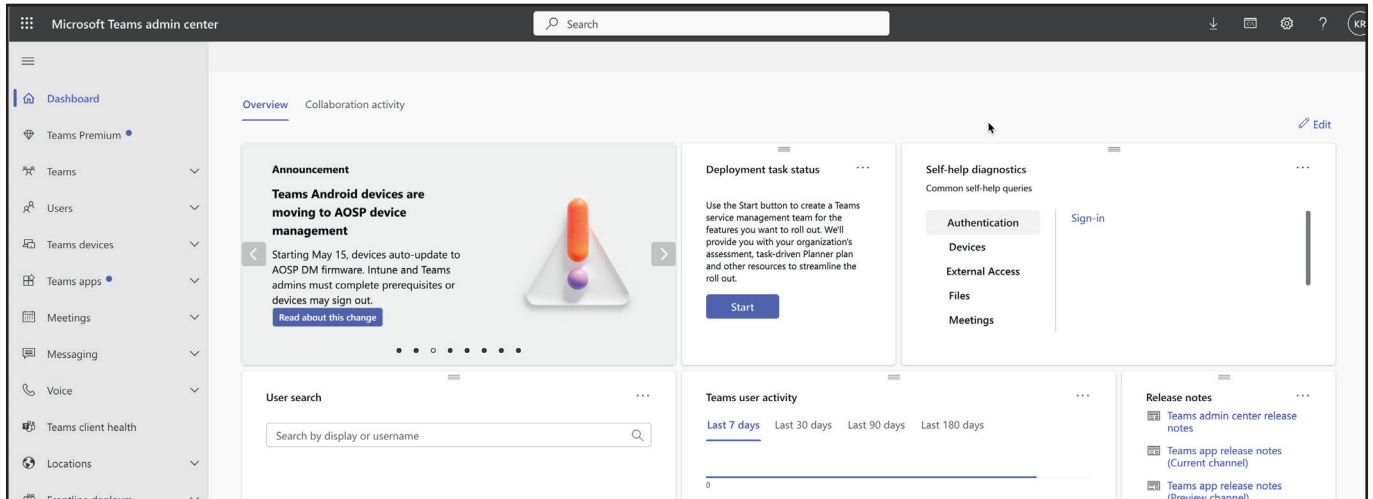
The installation of the CyberGate app for Microsoft Teams as described in this document makes the CyberGate app available for every user in the organisation. Of course this can be modified by selecting different user groups and / or setup policies to match the policies of your organisation.



# A Installation

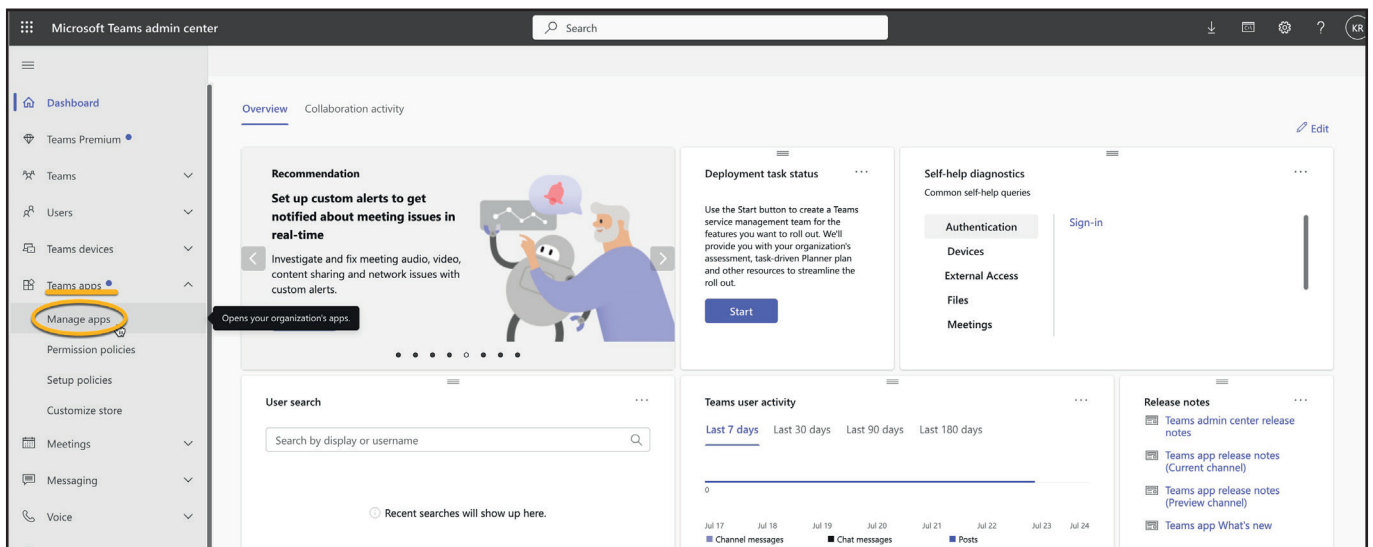
## How to install

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



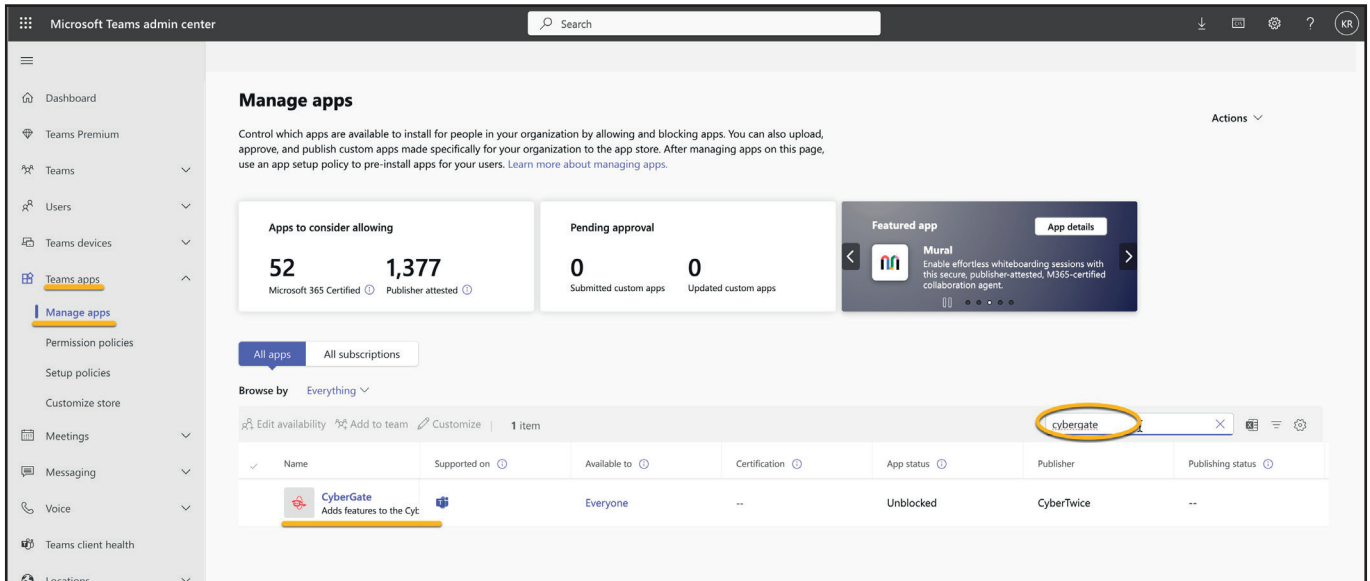
Microsoft Teams Admin Portal - Dashboard

- Navigate to the menu Teams apps - Manage apps



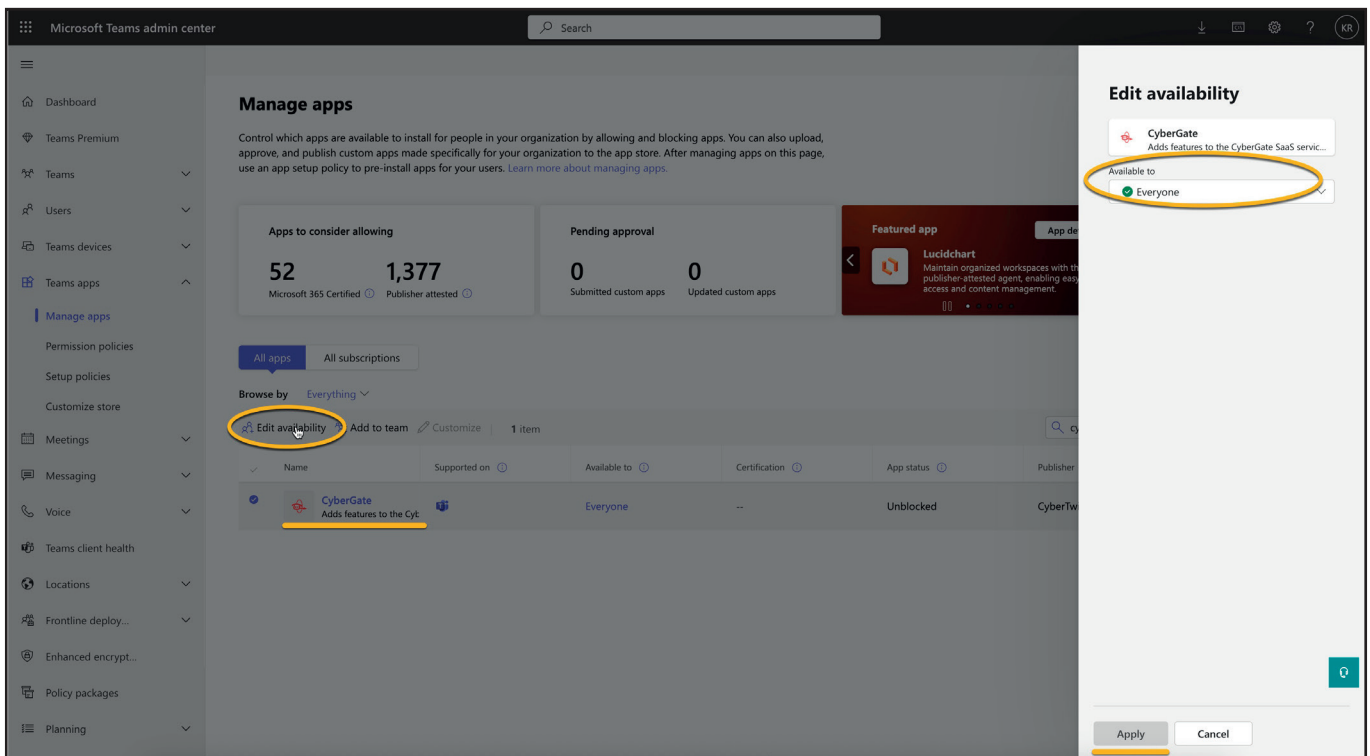
Microsoft Teams Admin Portal - Teams apps - Manage apps

- 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

Microsoft Teams admin center

### App setup policies

App setup policies control how apps are made available to a user with the Teams app. Use the Global (Org-wide default) policy and customize it or create custom policies and assign them to a set of users.

**App setup policies summary**

2 Default policies    0 Custom policies

Manage policies    Group policy assignment

Opens your app setup 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)'

Microsoft Teams admin center

### App setup policies

App setup policies control how apps are made available to a user with the Teams app. Use the Global (Org-wide default) policy and customize it or create custom policies and assign them to a set of users.

**App setup policies summary**

2 Default policies    0 Custom policies

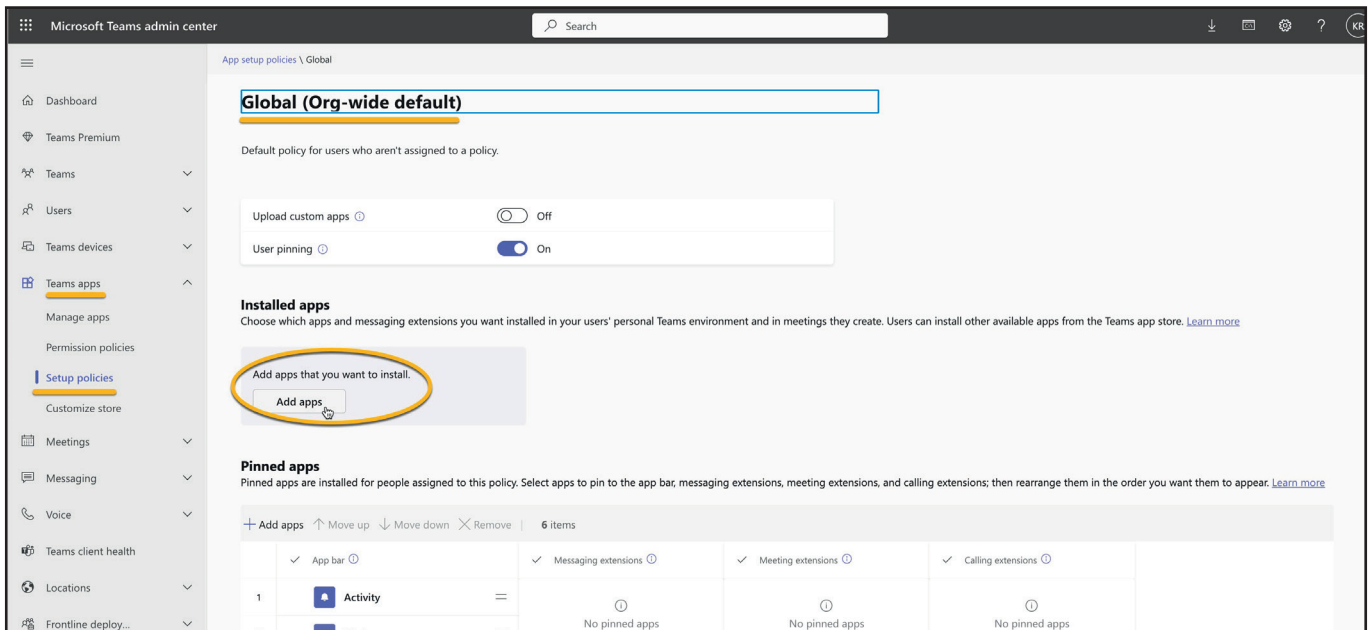
Manage policies    Group policy assignment

Opens your app setup policies.

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

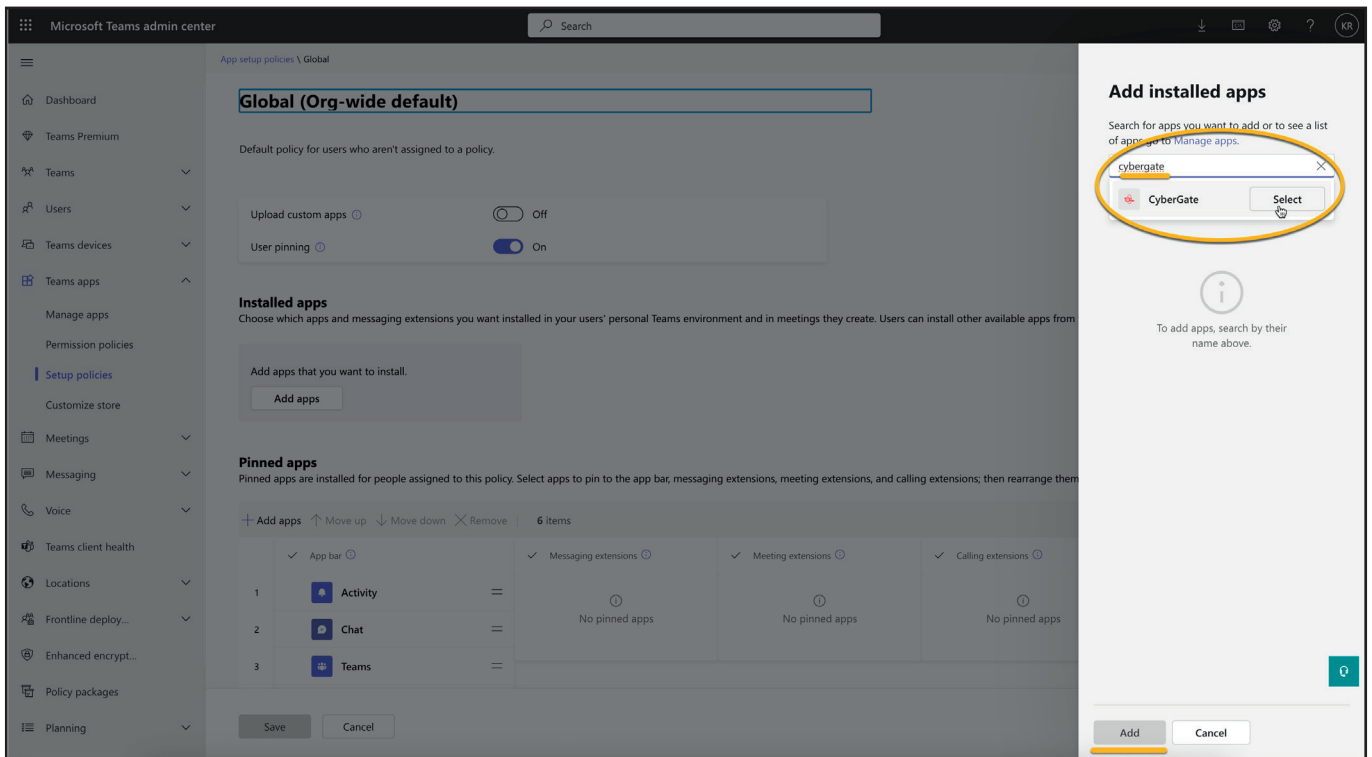
Microsoft Teams Admin Portal - Teams apps - Setup policies - Select 'Global'

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



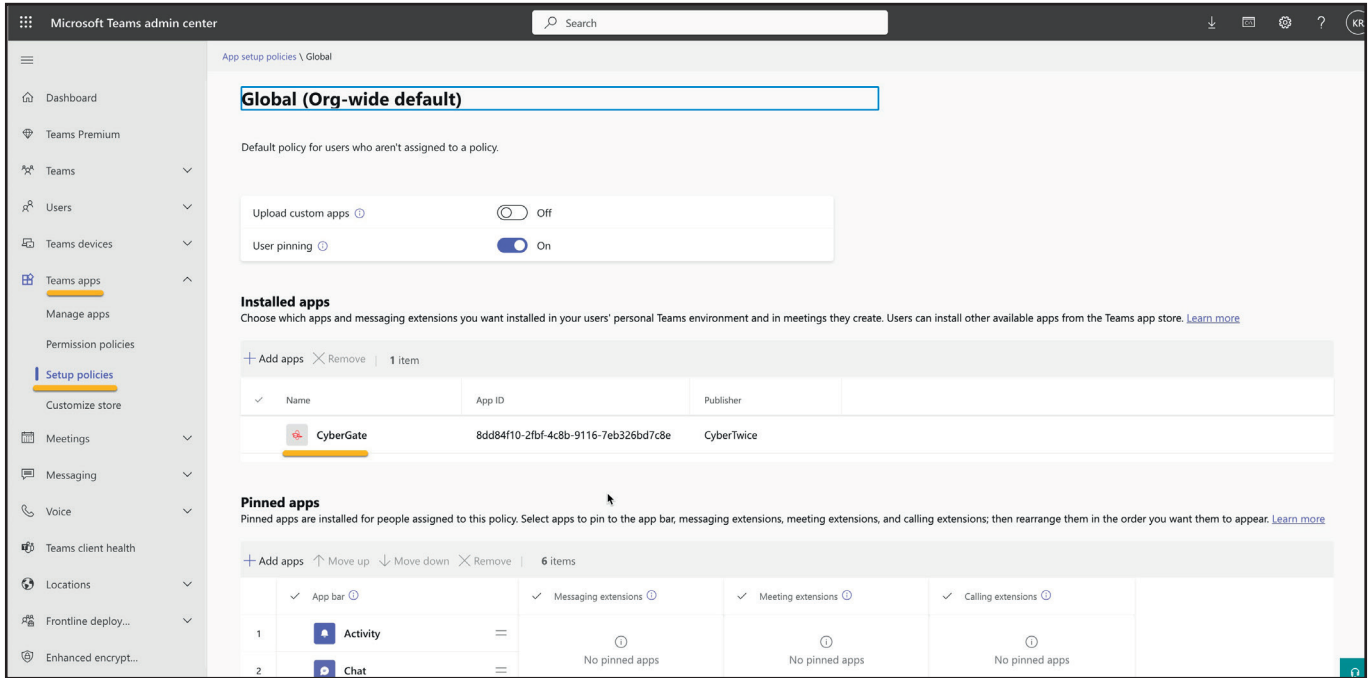
Microsoft Teams Admin Portal - Teams apps - Setup policies - Add apps

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



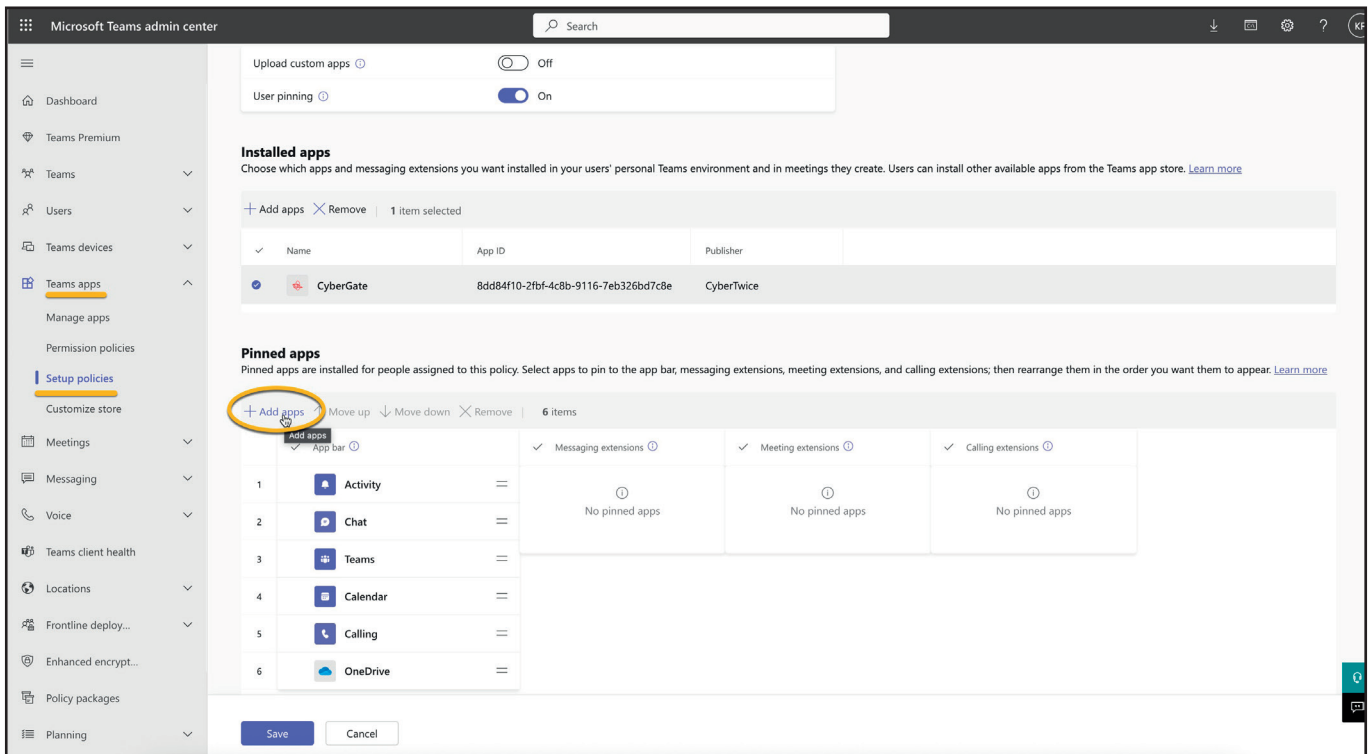
Microsoft Teams Admin Portal - Teams apps - Setup policies - Installed - Search and select CyberGate

The CyberGate app will show as installed.



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.



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 shows the Microsoft Teams Admin Portal interface. The main content area is titled "Pinned apps" and displays a list of pinned apps. The "Add pinned apps" dialog is open on the right side, showing a search box with "cybergate" entered. The search results show "CyberGate" with a "Select" button next to it. The "Add" button at the bottom of the dialog is highlighted.

**Installed apps**

Name	App ID	Publisher
CyberGate	8dd84f10-2fbf-4c8b-9116-7eb326bd7c8e	CyberTwice

**Pinned apps**

App bar	Messaging extensions	Meeting extensions	Calling extensions
1 Activity	No pinned apps	No pinned apps	No pinned apps
2 Chat	No pinned apps	No pinned apps	No pinned apps
3 Teams	No pinned apps	No pinned apps	No pinned apps
4 Calendar	No pinned apps	No pinned apps	No pinned apps
5 Calling	No pinned apps	No pinned apps	No pinned apps
6 OneDrive	No pinned apps	No pinned apps	No pinned apps

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 for configuring app setup policies. The left-hand navigation pane includes sections like Dashboard, Teams Premium, Teams, Users, Teams devices, Teams apps, and Setup policies. The main content area is titled 'App setup policies \ Global' and shows the 'Global (Org-wide default)' policy. Under the 'Default policy for users who aren't assigned to a policy' section, the 'Upload custom apps' and 'User pinning' toggle switches are both set to 'On'. The 'Installed apps' section shows a table with one entry: CyberGate (App ID: 8dd84f10-2bf-4c8b-9116-7eb326bd7c8e, Publisher: CyberTwice). The 'Pinned apps' section shows a list of 10 items, with CyberGate pinned to the App bar and the Calling extensions section.

Name	App ID	Publisher
CyberGate	8dd84f10-2bf-4c8b-9116-7eb326bd7c8e	CyberTwice

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

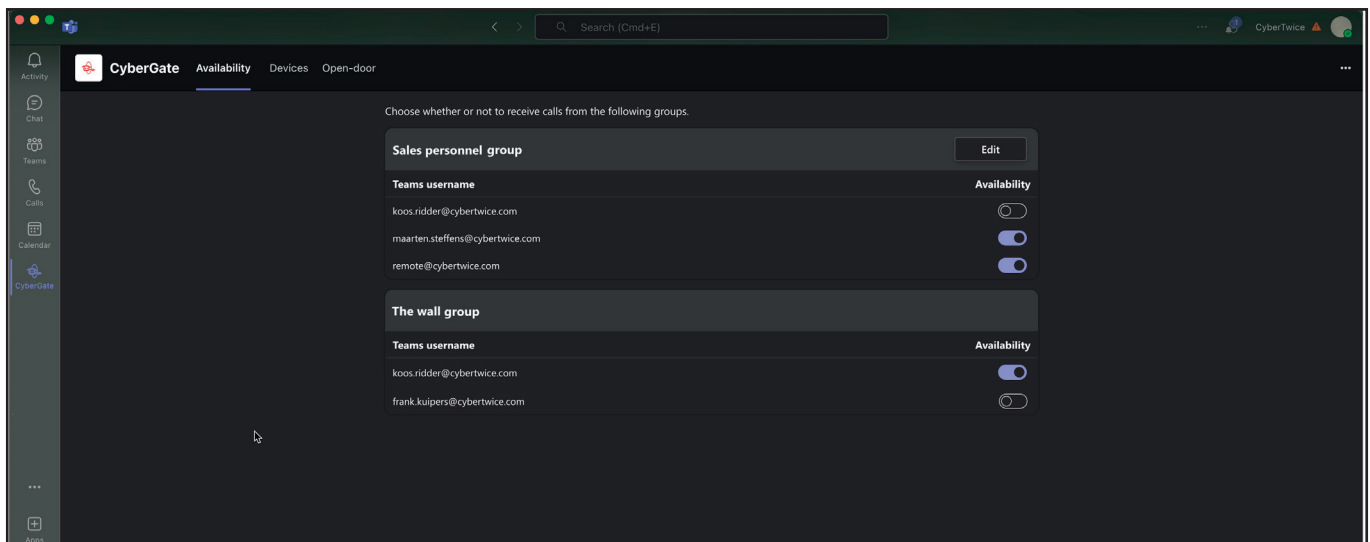
The 'Sale personnel group' contains three users and the 'The wall group' contains two users.

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](http://admin.cybergate.cybertwice.com)).

## Devices

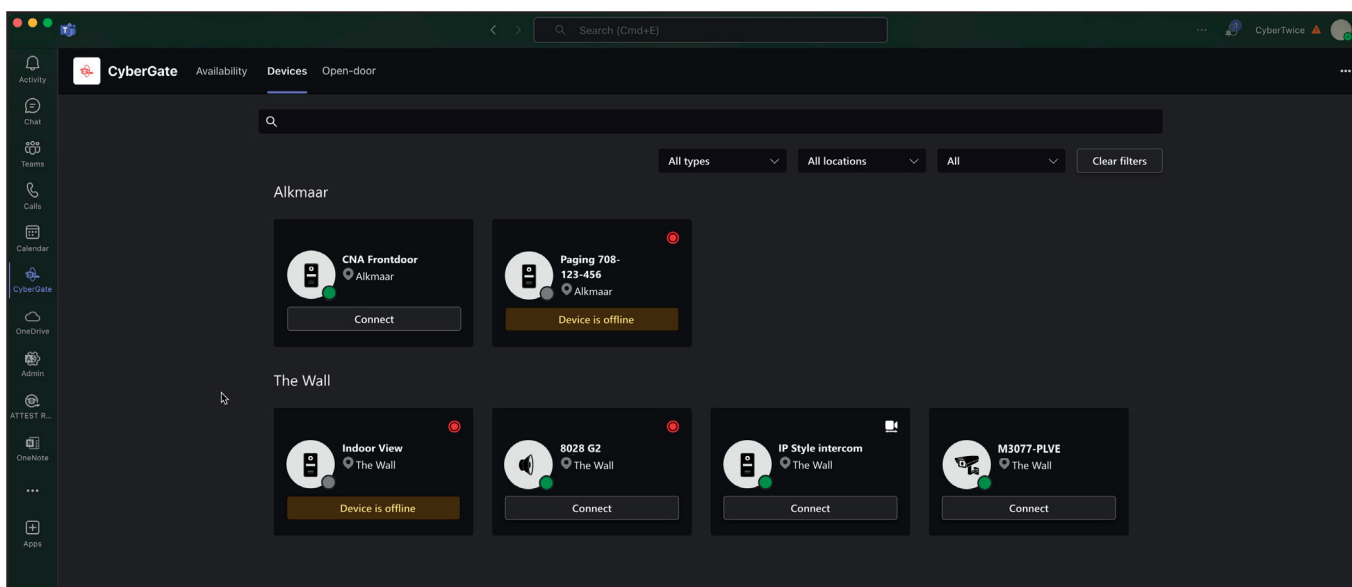
### How to use

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](http://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
<b>Test location</b>						
Test device	QV9ZTCASCUSHH0A5CHFA	AZZ ●●●●●●●●	yes	no	yes	<a href="#">Edit</a> <a href="#">Delete</a>

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

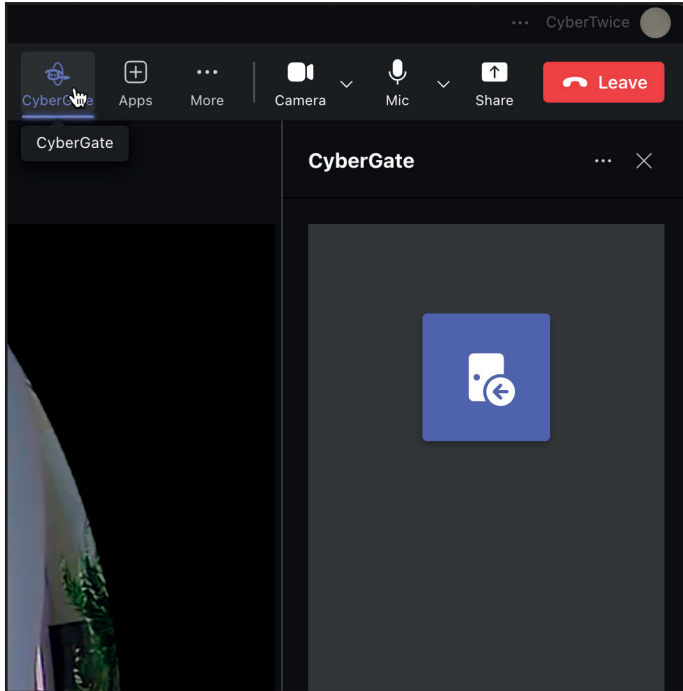
[Cancel] [Update]

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	06-10-2020	KR	Initial version
1.0.1	13-01-2021	KR	Added page numbers to the document and changed recipient SIP address (page 8)
1.0.2	26-08-2022	KR	Added Secure SIP chapter
1.0.3	18-09-2024	KR	Updated to use with AXIS OS 11
1.0.4	18-11-2024	KR	Fixed text and added "CyberGate app" appendix
1.0.5	02-05-2025	KR	Updated layout
1.0.6	13-08-2025	KR	Update CyberGate app section