



TechNote: Algo and CyberGate

Version: 1.0.6 ENG
Date: 21-08-2025



**Configure the Algo SIP Video
Intercom 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 Algo SIP 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>).

Algo SIP Video Intercom

For this document we used an Algo 8039 SIP Video Intercom (from now on named 'Algo') to connect to the CyberGate service (from now on named 'CyberGate').

Follow the next steps to configure the Algo 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 Algo

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

ALGO 8039 SIP Video Intercom Control Panel Firmware: 2.0.1

Status

Status and Login Video

Welcome to the Algo 8039 SIP Video Intercom Control Panel

Setting up your SIP Video Intercom:

Step 1: Configure your SIP Video Intercom
Log in with the default password and use the Basic Settings pages to set up the basic information.

Step 2: Check network settings (Optional)
Use the Network page under the Advanced Settings tab to change network settings. The default setting for the device is to obtain its IP address from a DHCP server. Contact your Network System administrator if you plan to assign a static IP address, Mask, and Gateway to the device.

Step 3: Secure your SIP Video Intercom (Optional)
Use the Admin page under the Advanced Settings tab to change the administrator password.
⚠️ Changing the password is extremely important if the device is directly connected to a public network.

Step 4: Register your SIP Video Intercom (Optional)
Please register your product using the link below:
<http://www.algosolutions.com/register>

Registration ensures your access to the latest upgrades to this product and important service notices.

Login

Password (default: algo)

Status	
Device Name	videodoorphone
SIP Registration	No Account
Call Status	Idle
Proxy Status	Single proxy mode
Security	TLS Disabled SRTP Disabled
Provisioning Status	None found
MAC	00:22:ee:0b:02:f1
IP	192.168.160.113
Netmask	255.255.255.0
Gateway	192.168.160.1
Date / Time	Fri Apr 15 09:12:08 UTC 2022
Multicast Mode	Disabled
Volume	Speaker Volume: 8 (-6dB)
Door Relay	Terminal Enabled, Door Locked
Network Door Controller	Not Configured
Extension to Dial	Not Configured

When signed-in successfully, the first menu shown is the Basic Settings-SIP menu.

ALGO 8039 SIP Video Intercom Control Panel Firmware: 2.0.1

Status **Basic Settings** Advanced Settings System Logout

SIP Features Video Keypad Door Control Multicast

SIP Settings

SIP

ⓘ This section allows the SIP server information & account credentials to be entered. This information should be obtained from your telephone system administrator or hosted account provider. After saving these settings, see the [Status](#) tab to confirm successful registration.

SIP Domain (Proxy Server)
 ⓘ Default port is 5060. To specify a different port, enter PROXY:PORT, e.g. my_proxy.com:5070, or 192.168.1.10:5080.

SIP Extension

Authentication ID

Authentication Password ⓘ

Display Name (Optional)

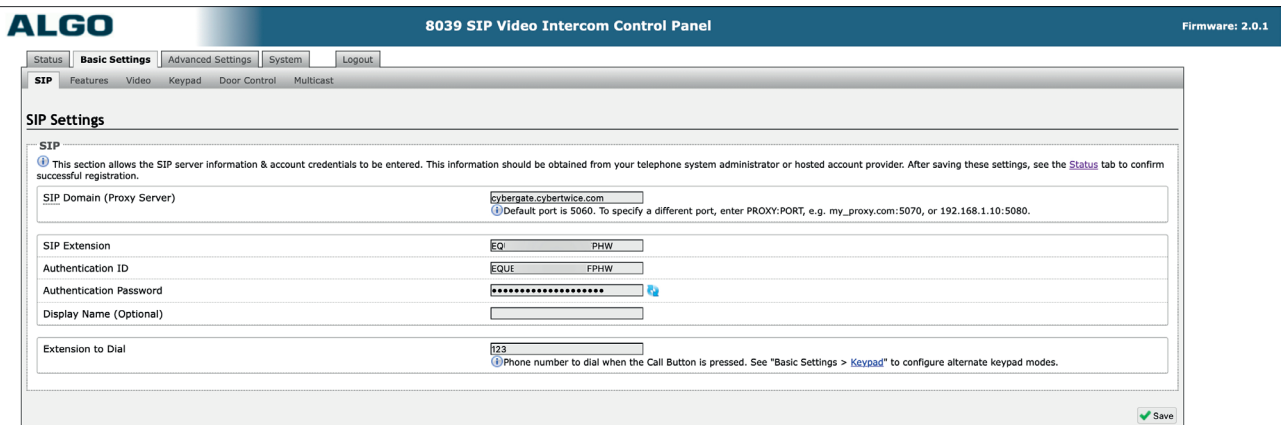
Extension to Dial
 ⓘ Phone number to dial when the Call Button is pressed. See "Basic Settings > Keypad" to configure alternate keypad modes.

Provide the following information:

SIP	
SIP Domain	cybergate.cybertwice.com
SIP Extension	Use the Username provided by the CyberGate Management Portal
Authentication ID	Use the Username provided by the CyberGate Management Portal
Authentication Password	Use the Password provided by the CyberGate Management Portal
Extension to Dial *	123

* The Extension to Dial is the default numer to dial when the 'Call' button on the Algo is pushed.

Click the Save button when done.



Navigate to the menu Basic settings-Video and change the following information:

SIP Video Settings	
SIP Video Capacity	Change to Auto
SIP Video Stream	Change to Auto Negotiation

Click the Save button when done.

ALGO 8039 SIP Video Intercom Control Panel Firmware: 2.0.1

Basic Settings | Video | Keypad | Door Control | Multicast

Video Settings

Camera Settings

- Exposure Region: Centre Weighted
- Camera View: Dewarped View
- White Balance: Auto
- Brightness: Default
- Contrast: Default
- Sharpness: Default
- Saturation: Default
- Powerline Frequency: 60 Hz (e.g. North America)
- Allow PTZ Video via DTMF Control:
 - Enabled (selected) / Disabled
 - Allows the web video and H.264 video stream to be controlled by DTMF commands on the receiving phone during a SIP call. This implements PTZ (Pan-Tilt-Zoom) via cropping the image when in low resolution mode. When enabled, press '*' followed by:
 - '1' - FullView Letterbox; '2' - Pan-Up; '3' - Fisheye Letterbox;
 - '4' - Pan-Left; '5' - Crop Center; '6' - Pan-Right;
 - '7' - Full Height; '8' - Pan-Down Fisheye; '9' - Full Fisheye.

H264 Streams

- Packetization Mode / Packet Type: Auto
- CIF Stream Bitrate: 600 kbps (default)
- HD Channel Resolution: 720p (1280x720)
- HD Channel Bitrate: 4 mbps (default)

SIP Video Settings

- Request Media Bandwidth: Enabled / Disabled
 - This controls if the 8039 adds RFC 3890 bandwidth modifiers and attributes, including "TIAS", "AS", and "maxprate" in the SDP offer/answer.
- SIP Video Capacity: Auto (CBP/CIF + HiP/High Res)
 - This controls the video parameters included in the SDP offer/answer. Manually specify the resolution only for legacy video phones with limited video SDP negotiation capabilities.
 - CBP: Constrained Baseline Profile; HiP: High Profile; CIF: 352x288; High Resolution: Defined by "HD Channel Resolution" parameter.
- Video Direction in SDP:
 - SDP Attribute "sendonly" / SDP Attribute "sendrecv"
 - The 8039 can only send out (but not receive) a video stream. Enable "sendrecv" mode only for legacy video phones with limited video SDP negotiation capabilities.
- SIP Video Stream: Auto Negotiation
 - This controls the actual video stream sent by the 8039. Manually specify the resolution only for legacy video phones with limited video SDP negotiation capabilities.

Web Video Settings

- Maximum Browser Sessions: 8
- Session Passcode: []
- This allows a separate password to be configured that allows access to only the "Status > Video" tab.

Save

Navigate to the menu Advanced Settings - Advanced SIP.

ALGO 8039 IP Video Multiline Intercom Firmware: 4.3.2

Navigation: Status | Basic Settings | **Advanced Settings** | System | Logout

Sub-navigation: Network | Admin | Time | Provisioning | Advanced Audio | **Advanced SIP** | Advanced Multicast | Snapshot

Advanced SIP Settings

General

SIP Transportation:
Select Auto to check DNS NAPTR record, then try UDP/TCP.
 In TLS mode, if the SIP Server requires endpoints to be authenticated, a PEM file containing both a device certificate and a private key needs to be installed on the Algo device. Use the "System > File Manager" tab to upload a certificate file renamed to 'sipclient.pem' in the 'certs' folder.

SIPS Scheme: Enabled Disabled

Validate Server Certificate: Enabled Disabled
Validate the SIP server against common certificate authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the 'certs/trusted' folder.

SIP Outbound Support (RFC 5626): Enabled Disabled
Only enable this option if the SIP server supports RFC 5626.

Outbound Proxy:

Register Period (seconds):

SRTP

SDP SRTP Offer:
SIP video calls are not supported when SRTP is enabled.

NAT

Media NAT: None ICE STUN

Server Redundancy

Server Redundancy Feature (Multiple SIP Server Support): Enabled Disabled

Interoperability

Keep-Alive Method: None Double CRLF
This setting will enable sending periodic CRLF messages for both UDP and TCP connections.

Use Outgoing TLS port in SIP headers: Enabled Disabled
Use ephemeral port number from outgoing SIP TLS connection instead of listening port number in SIP Contact and Via headers. This is useful to connect the device to some local SIP servers, like Asterisk or FreeSWITCH.

Do Not Reuse Authorization Headers: Enabled Disabled
When enabled, all SIP authorization information from the last successful request will not be reused in the next request.

Allow Missing Subscription-State Headers: Enabled Disabled
When enabled, allow SIP NOTIFY messages that do not contain a "Subscription-State" header.

Save

Change the following information:

General

SIP Transportation

Change TCP

Click the Save button when done.

The screenshot shows the 'Advanced SIP Settings' page in the ALGO 8039 IP Video Multion Intercom web interface. The page is organized into several sections:

- General:**
 - SIP Transportation:** Set to 'Auto'. A tooltip explains: 'Select Auto to check DNS NAPTR record, then try UDP/TCP. In TLS mode, if the SIP Server requires endpoints to be authenticated, a PEM file containing both a device certificate and a private key needs to be installed on the Algo device. Use the "System > File Manager" tab to upload a certificate file renamed to "sipclient.pem" in the "certs" folder.'
 - SIPS Scheme:** Radio buttons for 'Enabled' and 'Disabled'.
 - Validate Server Certificate:** Radio buttons for 'Enabled' and 'Disabled'. A tooltip explains: 'Validate the SIP server against common certificate authorities. To validate against additional certificates, use the "System > File Manager" tab to upload a Base64 encoded X.509 certificate file in .pem, .cer, or .crt format to the "certs/trusted" folder.'
 - SIP Outbound Support (RFC 5626):** Radio buttons for 'Enabled' and 'Disabled'. A tooltip explains: 'Only enable this option if the SIP server supports RFC 5626.'
 - Outbound Proxy:** An empty text input field.
 - Register Period (seconds):** A text input field containing '6000'.
- SRTP:**
 - SDP SRTP Offer:** A dropdown menu set to 'Disabled'. A tooltip explains: 'SIP video calls are not supported when SRTP is enabled.'
- NAT:**
 - Media NAT:** Radio buttons for 'None', 'ICE', and 'STUN'.
- Server Redundancy:**
 - Server Redundancy Feature (Multiple SIP Server Support):** Radio buttons for 'Enabled' and 'Disabled'.
- Interoperability:**
 - Keep-Alive Method:** Radio buttons for 'None' and 'Double CRLF'. A tooltip explains: 'This setting will enable sending periodic CRLF messages for both UDP and TCP connections.'
 - Use Outgoing TLS port in SIP headers:** Radio buttons for 'Enabled' and 'Disabled'. A tooltip explains: 'Use ephemeral port number from outgoing SIP TLS connection instead of listening port number in SIP Contact and Via headers. This is useful to connect the device to some local SIP servers, like Asterisk or FreeSWITCH.'
 - Do Not Reuse Authorization Headers:** Radio buttons for 'Enabled' and 'Disabled'. A tooltip explains: 'When enabled, all SIP authorization information from the last successful request will not be reused in the next request.'
 - Allow Missing Subscription-State Headers:** Radio buttons for 'Enabled' and 'Disabled'. A tooltip explains: 'When enabled, allow SIP NOTIFY messages that do not contain a "Subscription-State" header.'

A 'Save' button is located at the bottom right of the settings area.

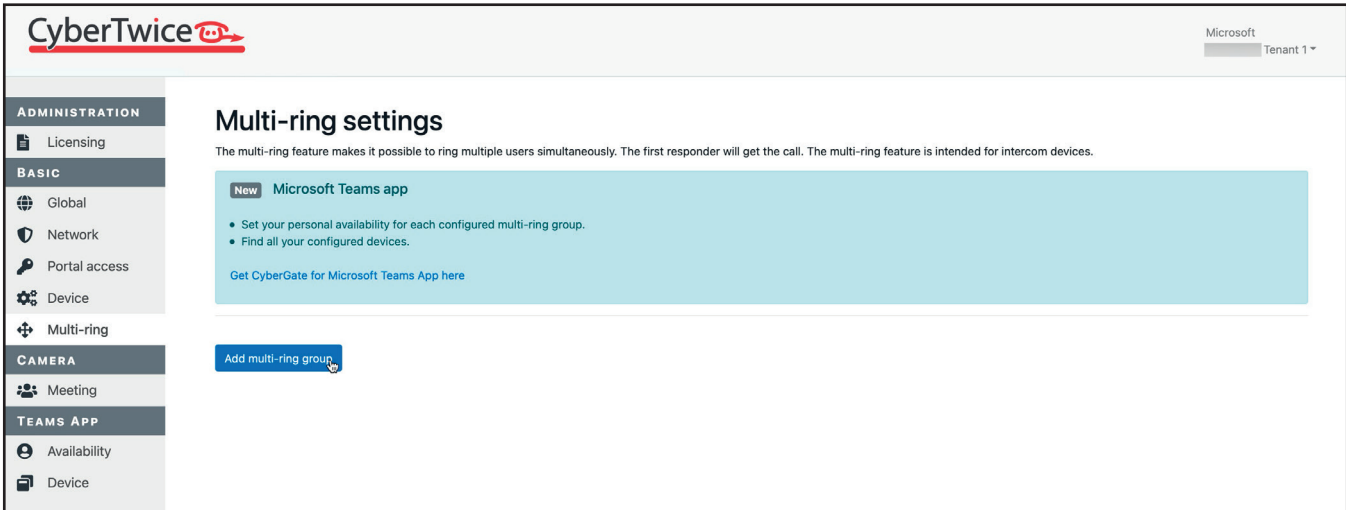
Configuration of the Algo is now finished.

Pressing the call button on the Algo will initiate a call to the number you've configured as 'Extension to Dial' in the Basic settings - SIP menu.

As this number (123) is not a valid Teams user within your Teams environment, you must configure a Multi-ring group via the CyberGate Management portal. The Multi-ring group enables you to 'translate' the dialed number (123) to one or more valid and existing Teams user(s).

Navigate to the following URL: <https://admin.cybergate.cybertwice.com>

Log in to the admin portal using a Microsoft account with admin privileges and navigate to the Multi-ring Settings menu.



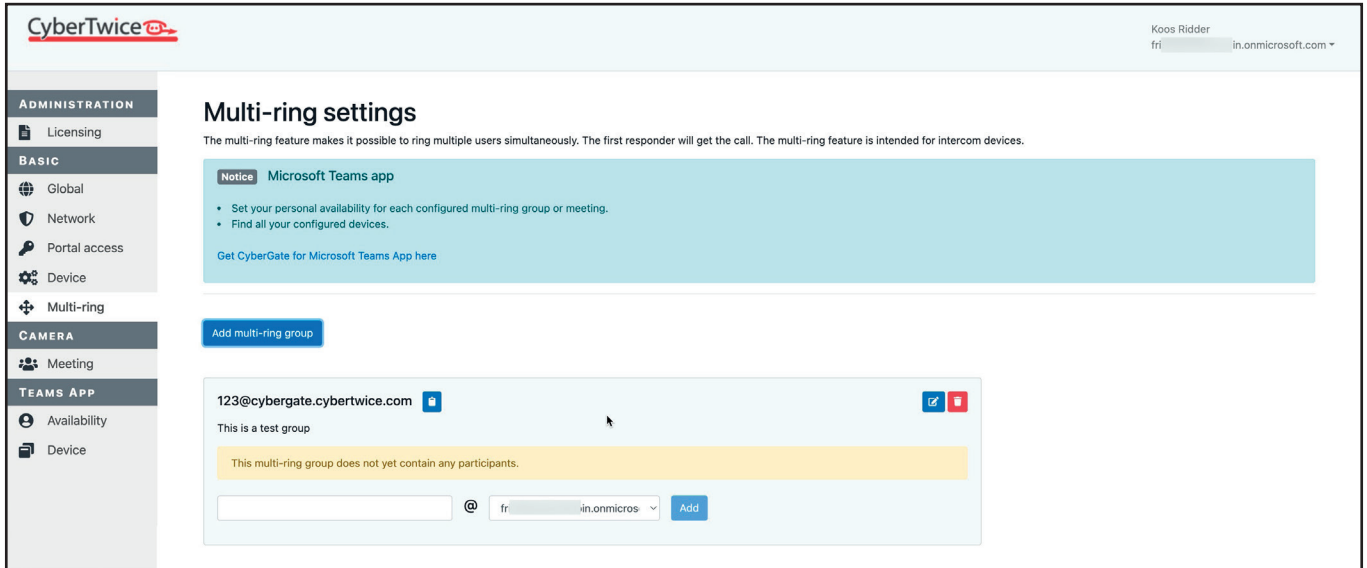
The screenshot shows the CyberTwice admin portal interface. The top left features the CyberTwice logo. The top right shows the user is logged in as 'Microsoft Tenant 1'. A left-hand navigation menu is visible with categories: ADMINISTRATION (Licensing), BASIC (Global, Network, Portal access, Device, Multi-ring), CAMERA (Meeting), and TEAMS APP (Availability, Device). The main content area is titled 'Multi-ring settings' and contains a 'New Microsoft Teams app' section with the following text: 'The multi-ring feature makes it possible to ring multiple users simultaneously. The first responder will get the call. The multi-ring feature is intended for intercom devices.' Below this are two bullet points: 'Set your personal availability for each configured multi-ring group.' and 'Find all your configured devices.' A link 'Get CyberGate for Microsoft Teams App here' is also present. At the bottom of the main content area, there is a blue button labeled 'Add multi-ring group'.

Click the blue 'Add multi-ring group' button and provide the following information:

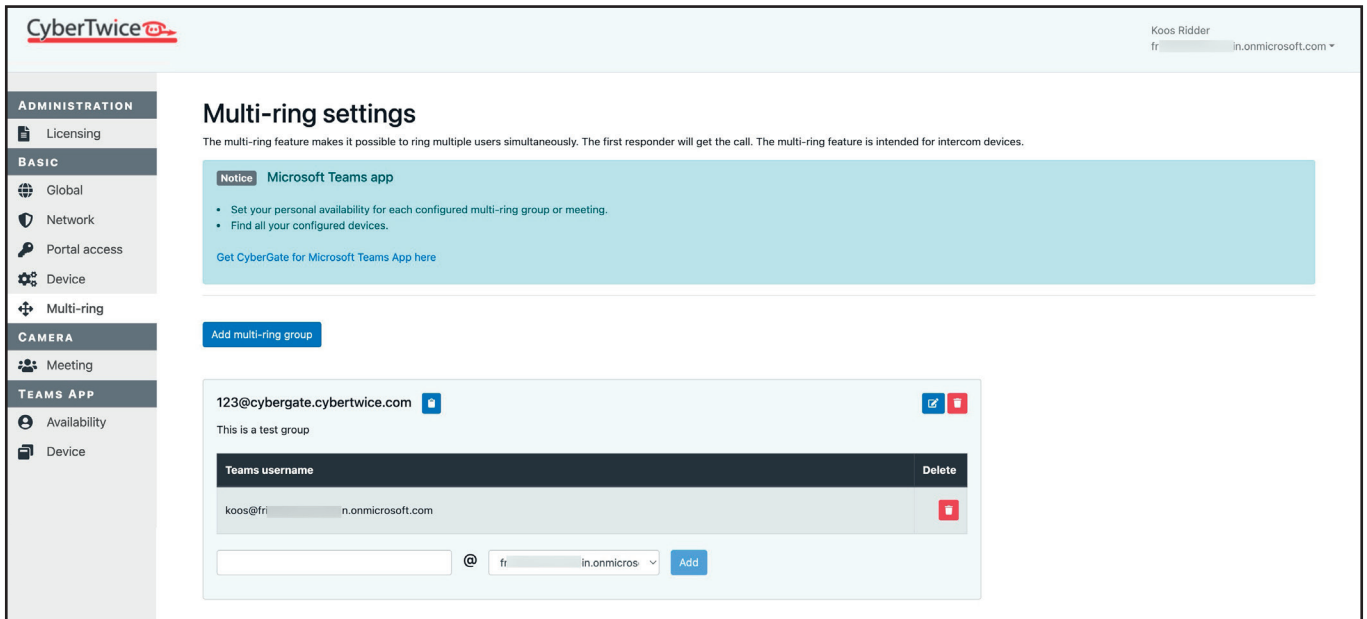
Name	Enter 123 (the number the Algo dials)
Description	Describe this Multi-ring group

Click the blue 'Save' button when done.

The Multi-ring group is now created.



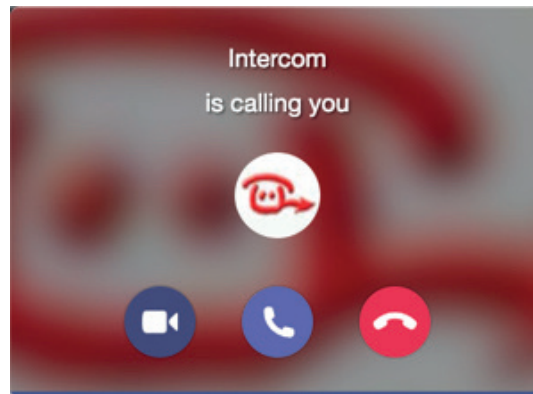
Add the person or persons you would like to be notified when a person rings the Algo. Use the first part of the Teams user name, so don't add the domain name as it will be added automatically.



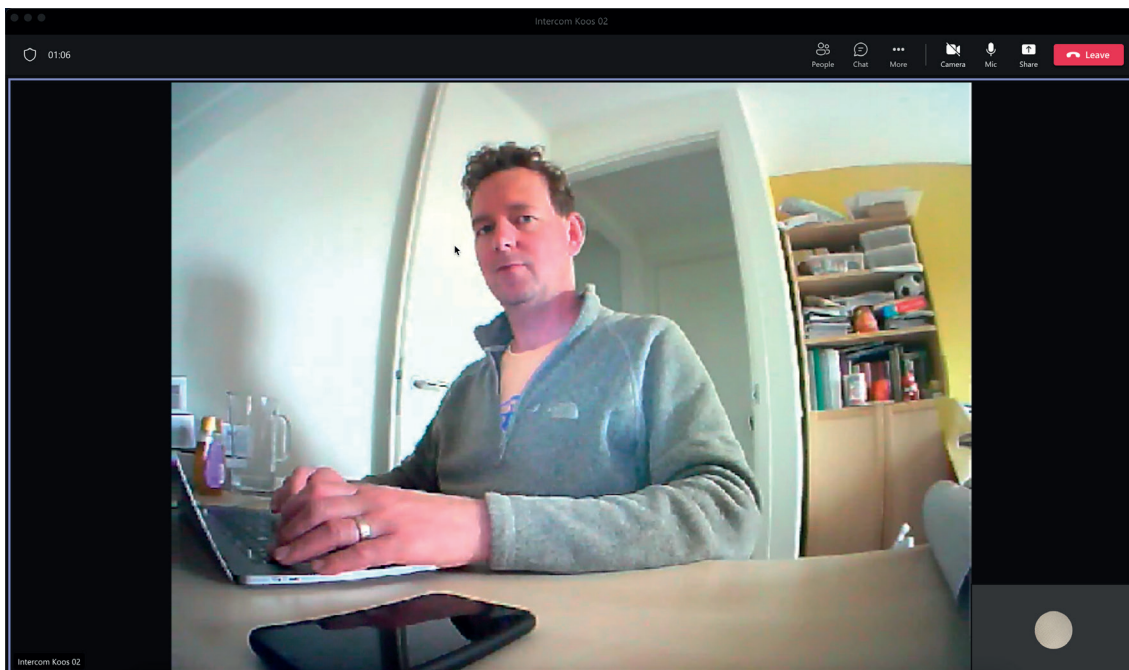
The configuration is now done.

The following sequence will take place when pressing the call button on the Algo:

- The Algo will place a call to the CyberGate using the number 123
- The CyberGate will answer the call to 123, recognizes the 123 number as a 'Multi-ring group'
- The CyberGate checks what Teams user(s) to call (as configured in the Multi-ring group) and will place the call to all Teams users in this group
- The first Teams user that answers the incoming call in Teams (by clicking the pick-up symbol) will be connected to the Algo



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 '6' code as configured in the Algo, this will trigger the relay in the Algo 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.

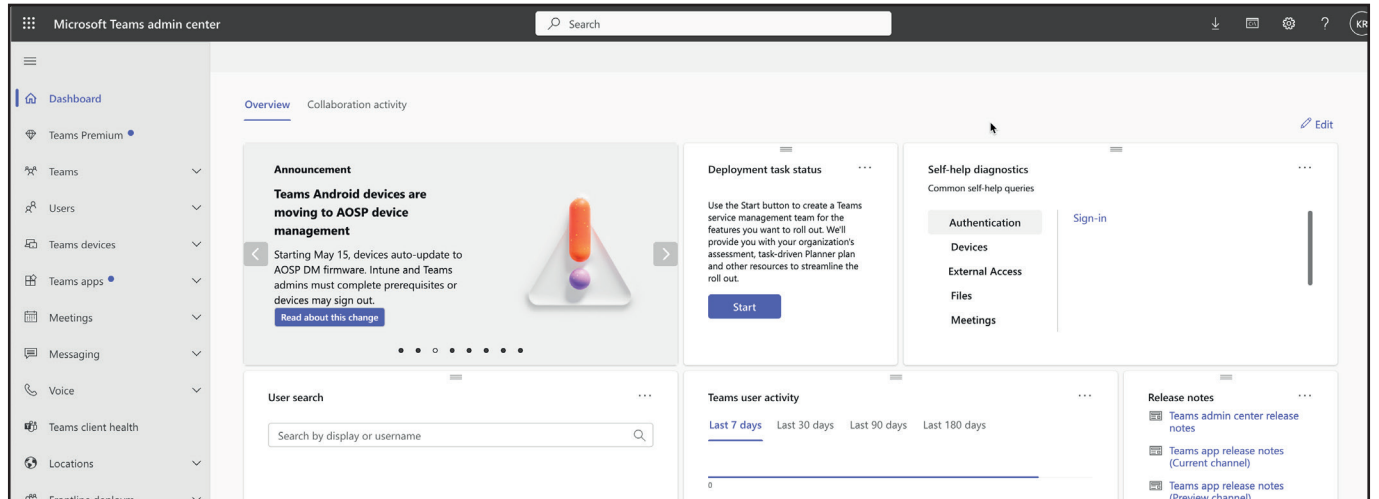
The installation of the CyberGate app for Microsoft Teams as described in this document makes the CyberGate app available for every user in the organisation. Of course this can be modified by selecting different user groups and / or setup policies to match the policies of your organisation.



Installation

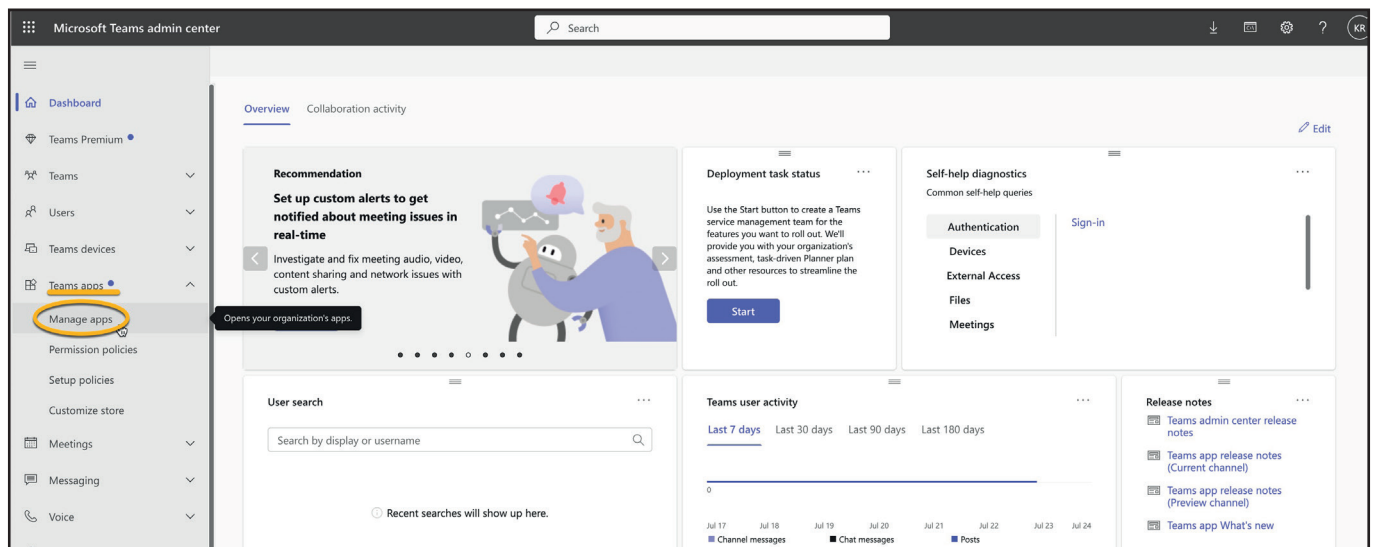
How to install

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



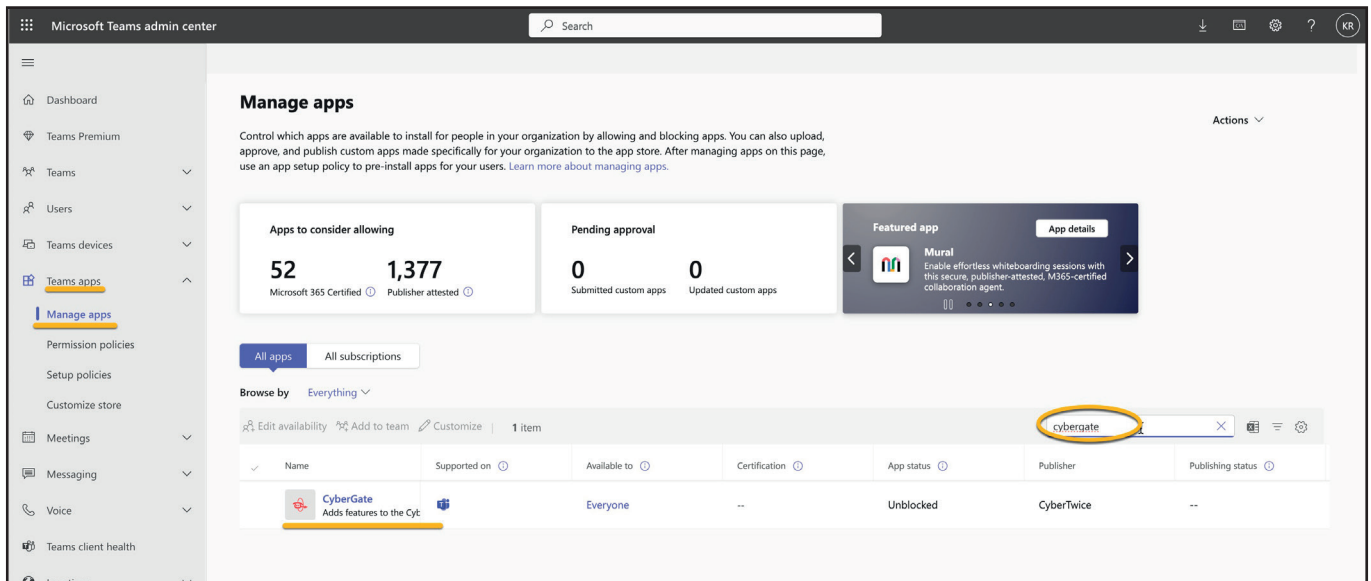
Microsoft Teams Admin Portal - Dashboard

- Navigate to the menu Teams apps - Manage apps



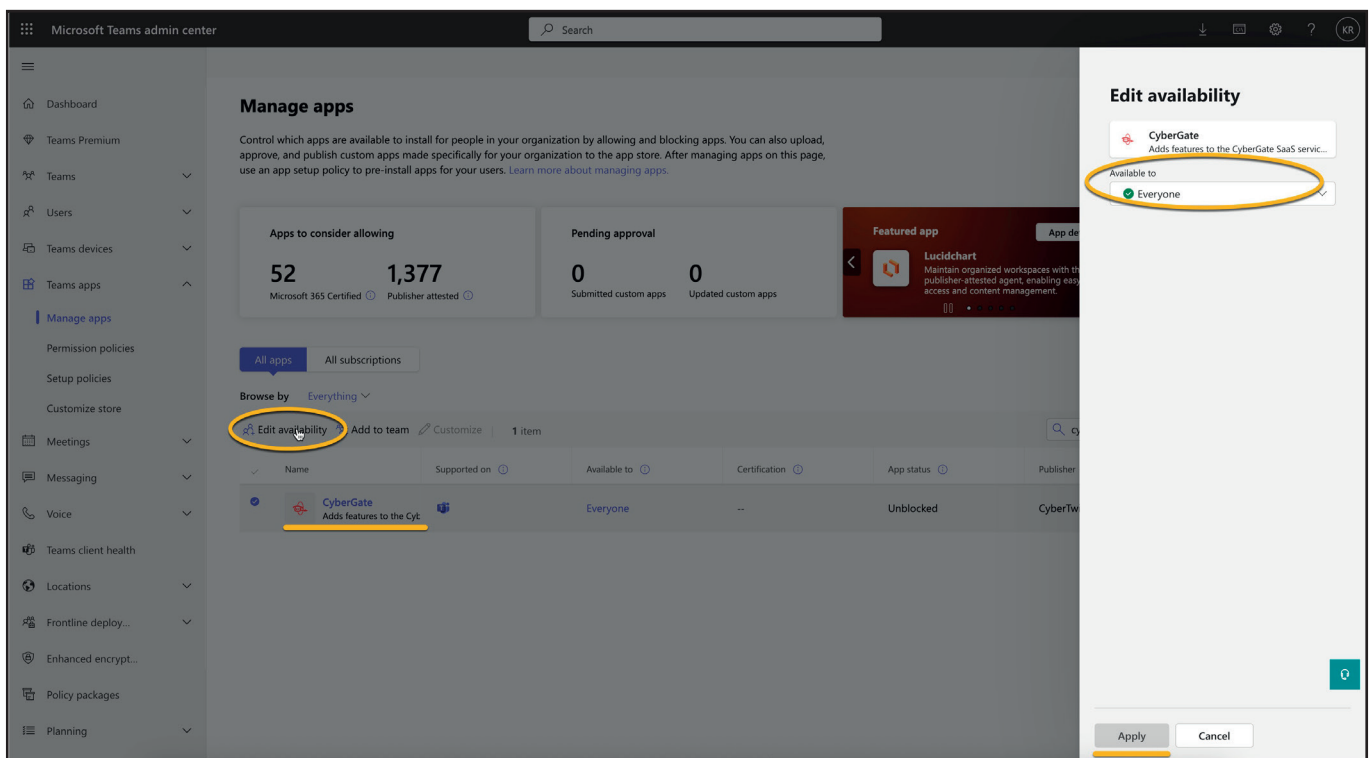
Microsoft Teams Admin Portal - Teams apps - Manage apps

- 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

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

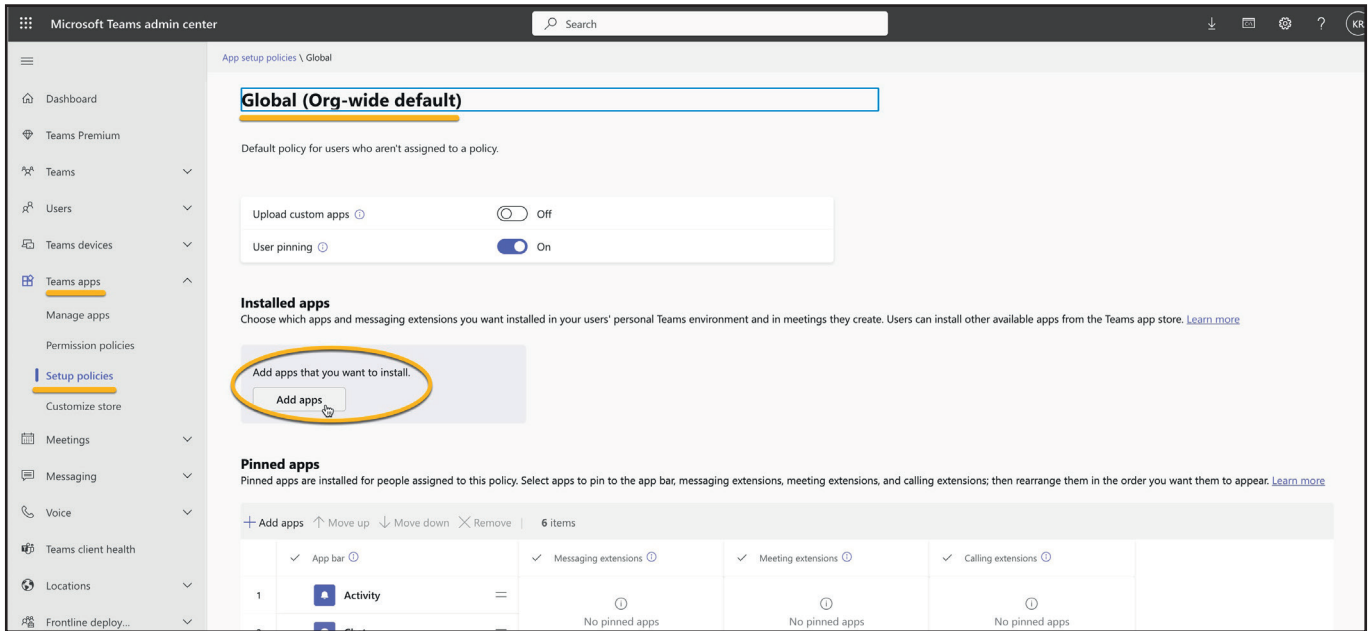
Manage policies Group policy assignment

Opens your app setup policies.

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

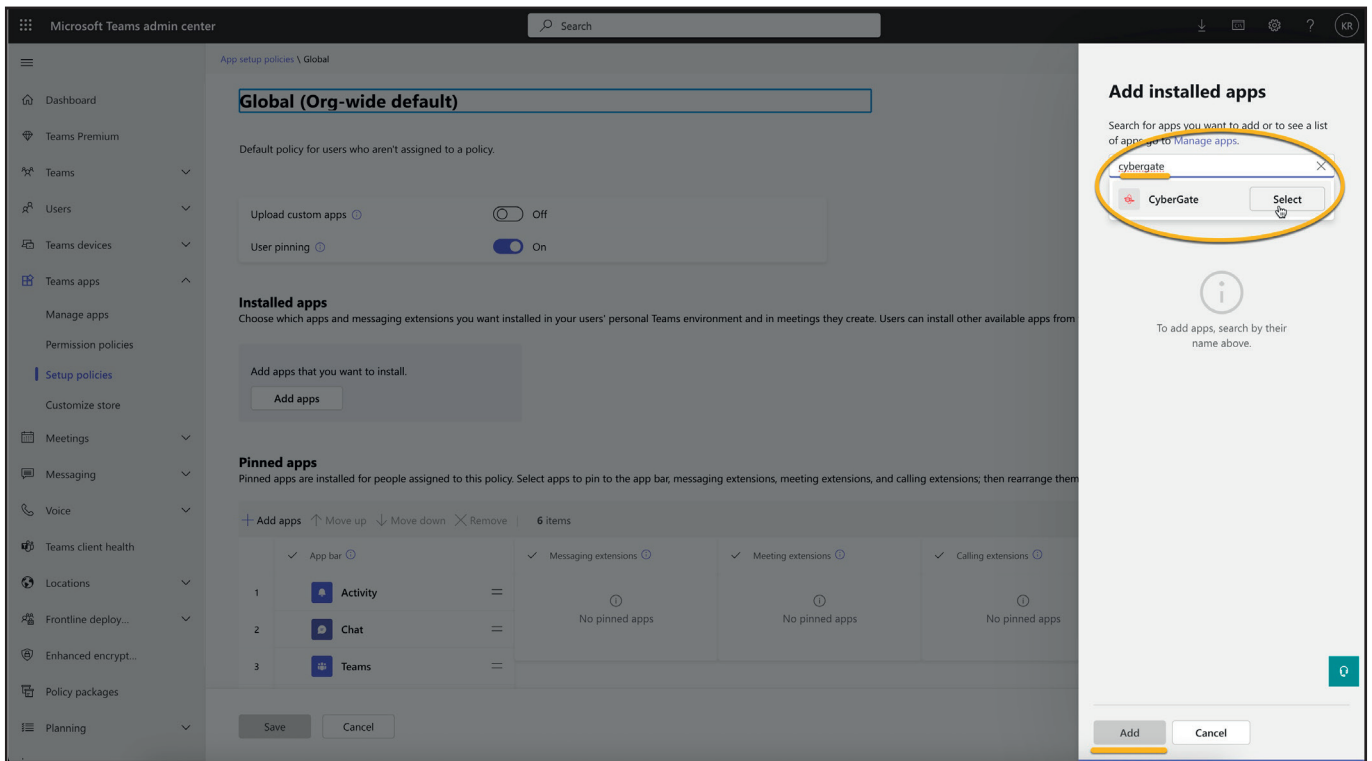
Microsoft Teams Admin Portal - Teams apps - Setup policies - Select 'Global'

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



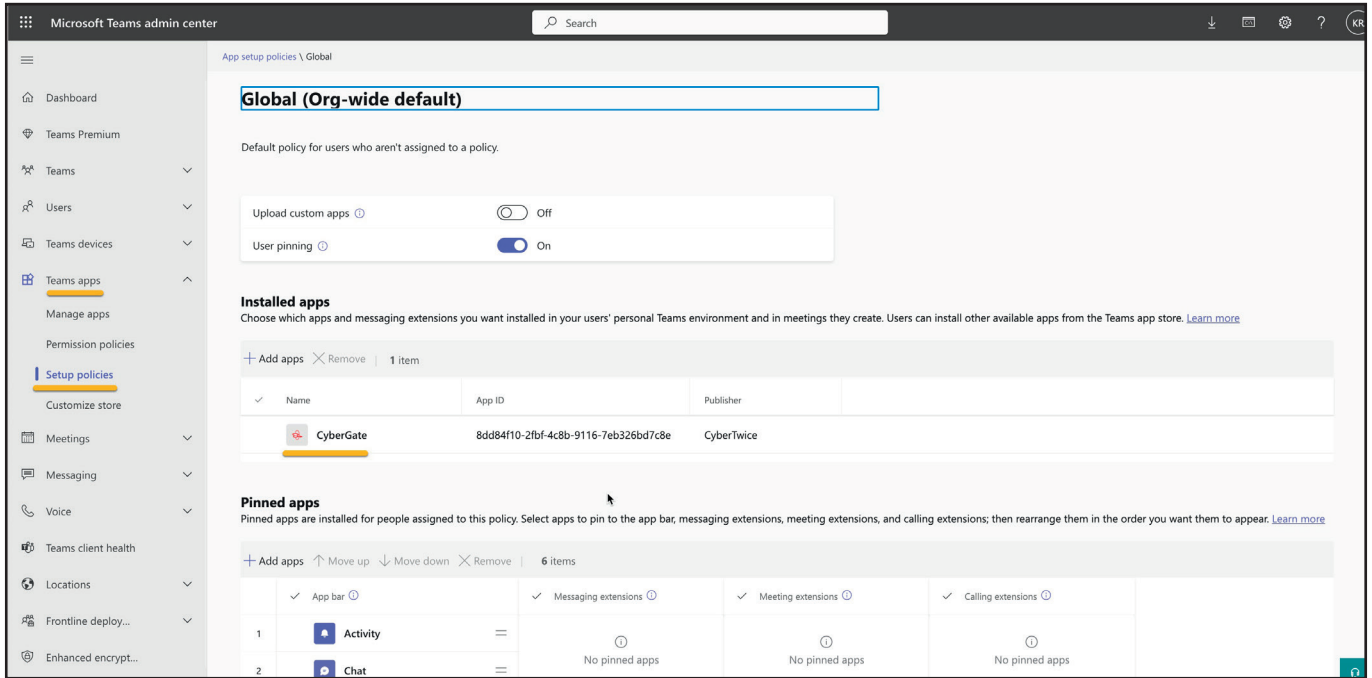
Microsoft Teams Admin Portal - Teams apps - Setup policies - Add apps

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



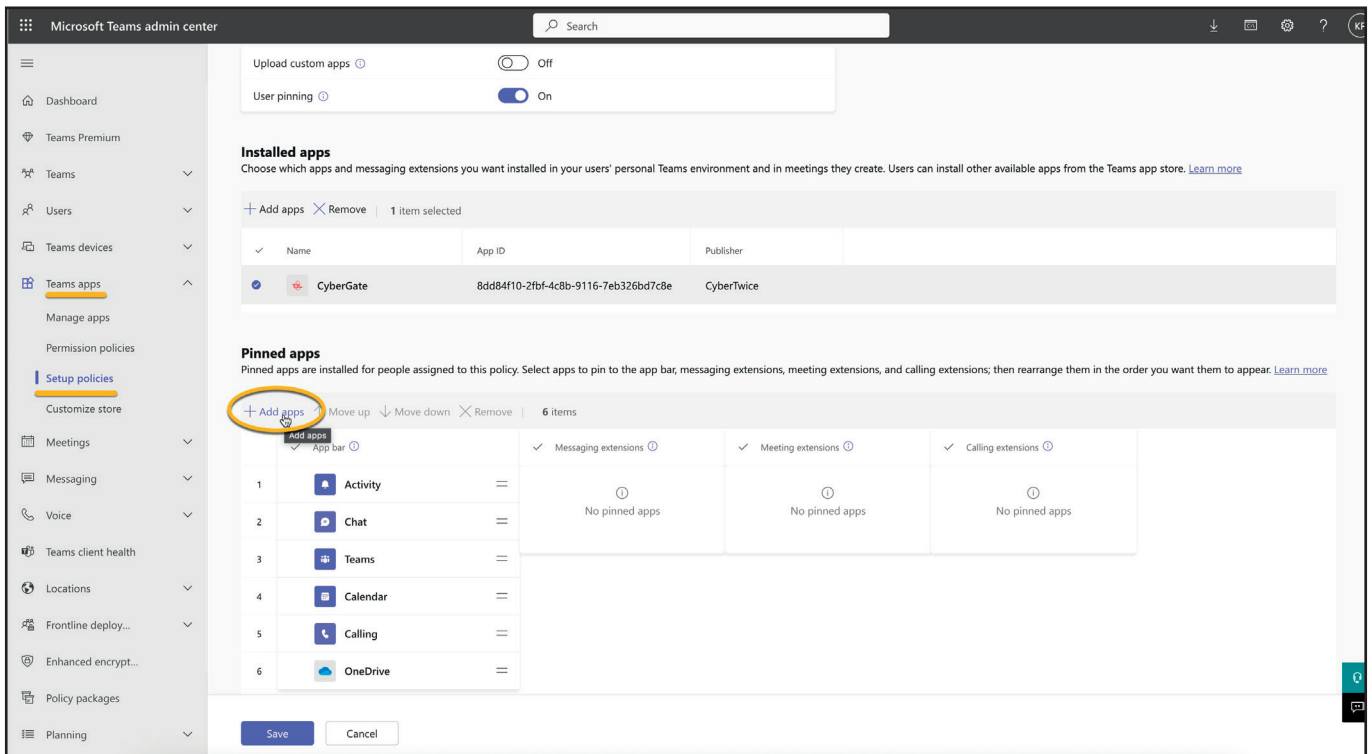
Microsoft Teams Admin Portal - Teams apps - Setup policies - Installed - Search and select CyberGate

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 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 modal is highlighted. In the background, the "Pinned apps" section is visible, showing a list of apps including 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 shows the Microsoft Teams Admin Center interface. The left sidebar contains navigation options 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 'Default policy for users who aren't assigned to a policy', the 'Upload custom apps' and 'User pinning' options 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 the CyberGate app pinned to the App bar, Calling extensions, and Meeting extensions.

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

App bar	Messaging extensions	Meeting extensions	Calling extensions
CyberGate	No pinned apps	No pinned apps	CyberGate

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

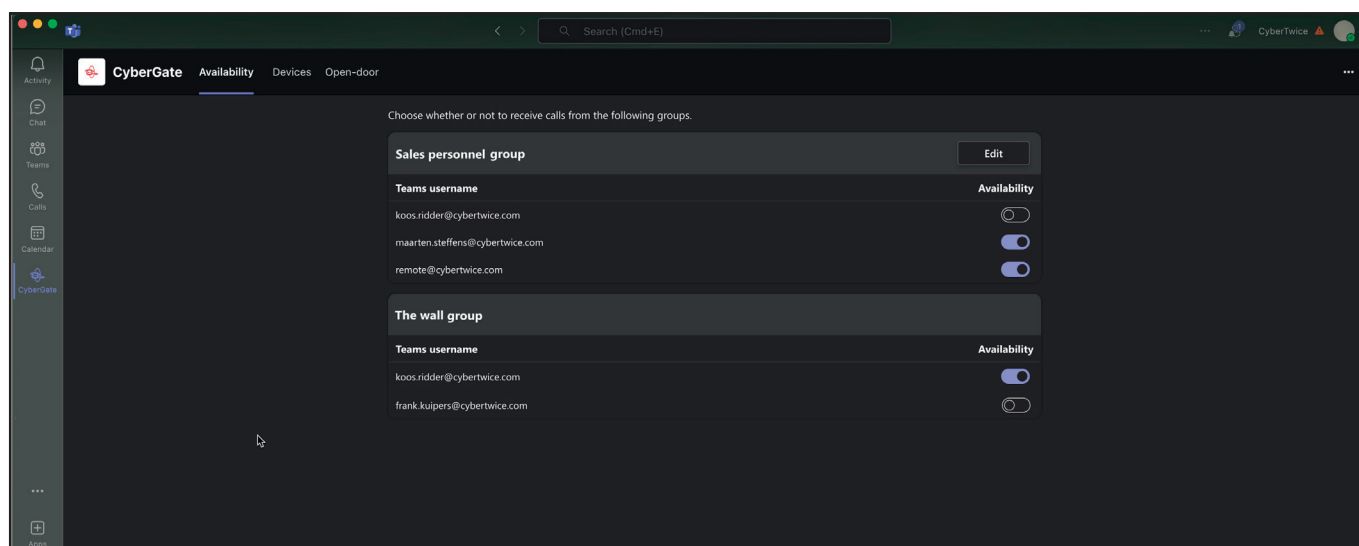
The 'Sale personnel group' contains three users and the 'The wall group' contains two users.

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

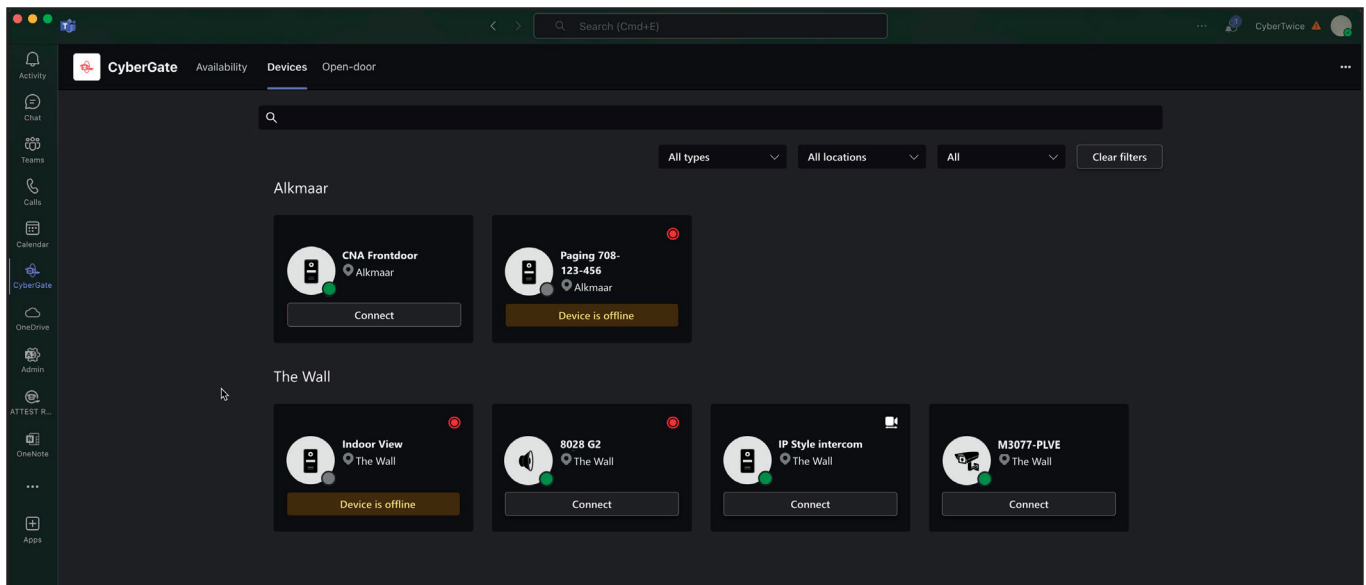
How to use

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

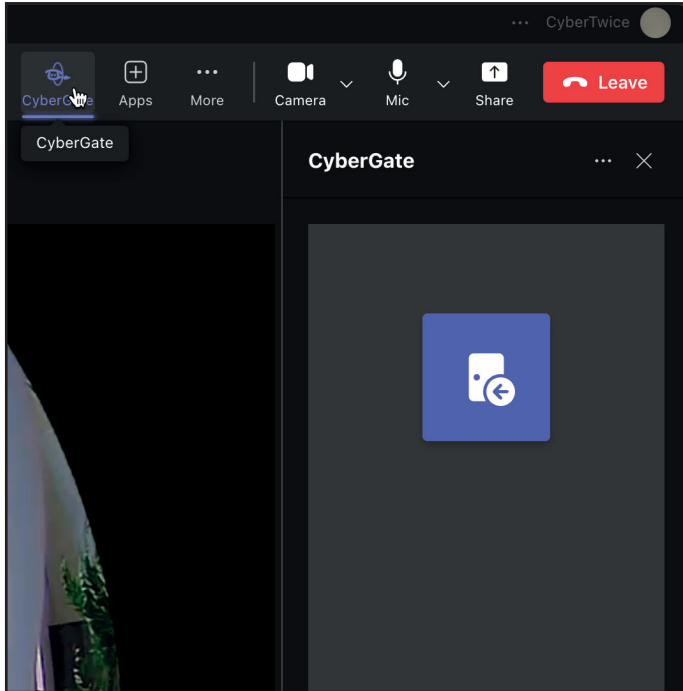
[Cancel] [Update]

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	15-04-2022	KR	Initial version
1.0.1	29-08-2022	KR	Modified transportation settings
1.0.2	08-10-2024	KR	Modified screenshots
1.0.4	13-11-2024	KR	Fixed text and added "CyberGate app" appendix
1.0.5	20-01-2025	KR	Modified video settings
1.0.6	21-08-2025	KR	Updated Appendix