

TechNote: Busch-Jaeger and CyberGate

Version: 1.0.0 ENG
Date: 30-07-2025



**Configure the Busch Welcome® IP
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 a Busch Welcome® IP 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>).



Busch Welcome® IP

For this document we used a Busch Welcome® IP with display (from now on named 'Outdoor Station') to connect to the CyberGate service (from now on named 'CyberGate').

The tested configuration also features a Smart Access Point Pro. The Outdoor Stations configuration is done from within the Smart Access Point Pro.

This document can be used for *all* Busch Welcome® IP Outdoor Stations. As the configuration for the Outdoor stations without display differs slightly from Outdoor stations with display both types are described in this manual.

Please upgrade the Outdoor Station to the latest available firmware!



Secure communication with CyberGate.

The Outdoor Stations are certified for secure communication with 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

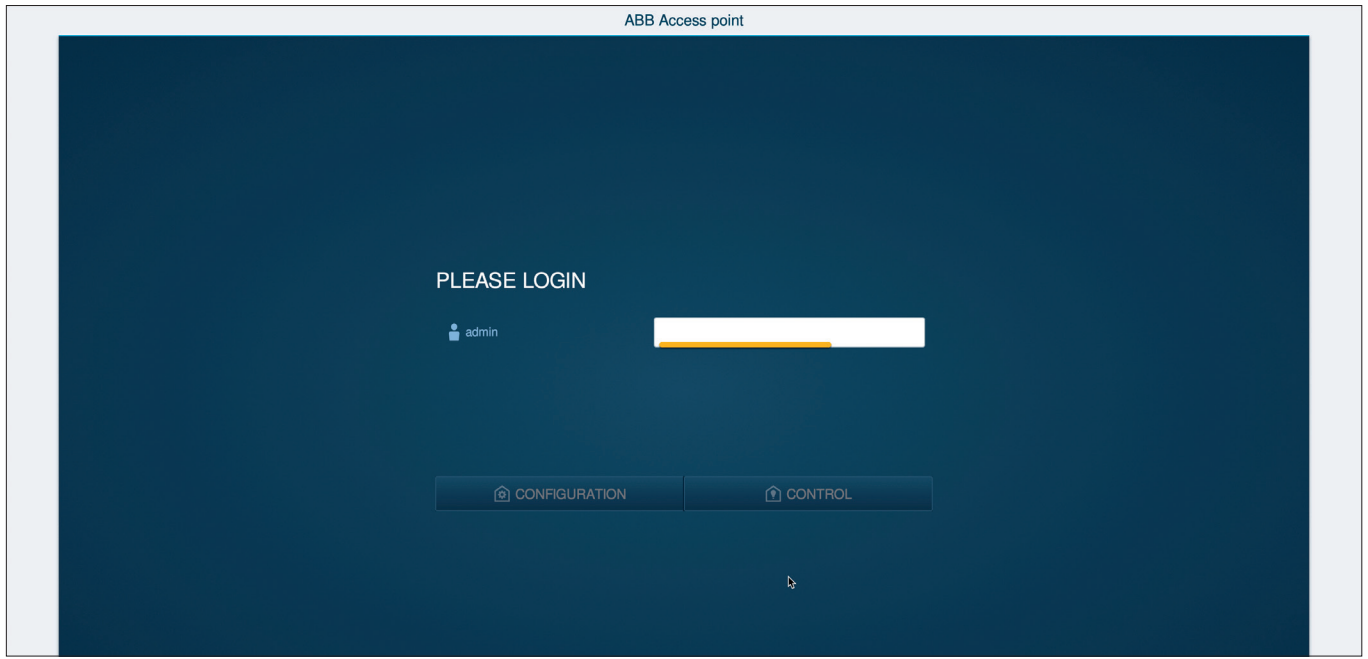
Installation of the CyberGate app for Microsoft Teams is highly recommended.

Follow the next steps to configure the Outdoor Station to connect to CyberGate.

Connect the Outdoor Station

Connect the Outdoor Station to the network, power it on. To configure the Outdoor Station, log in to the Smart Access Point Pro webinterface.

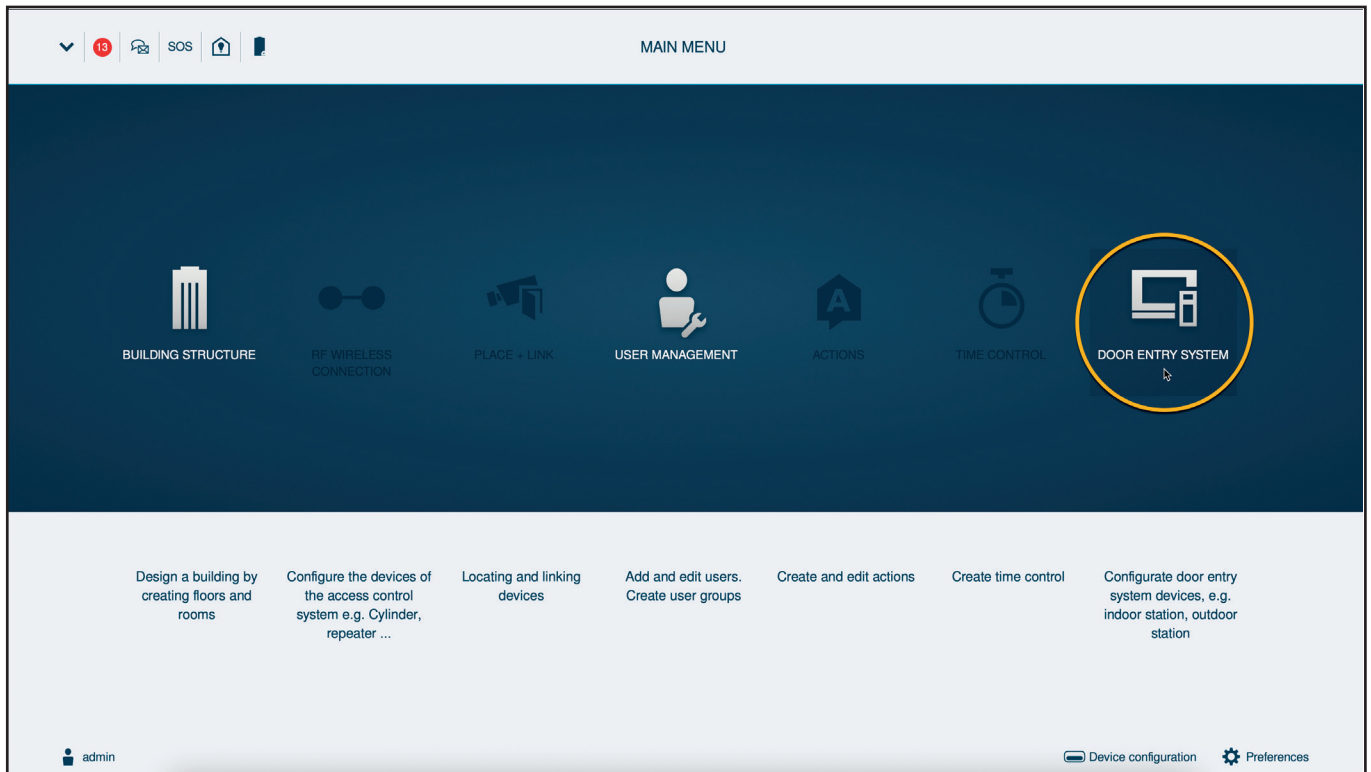
Sign in with the configured or supplied password of the Smart Access Point Pro.



Smart Access Point Pro - Login

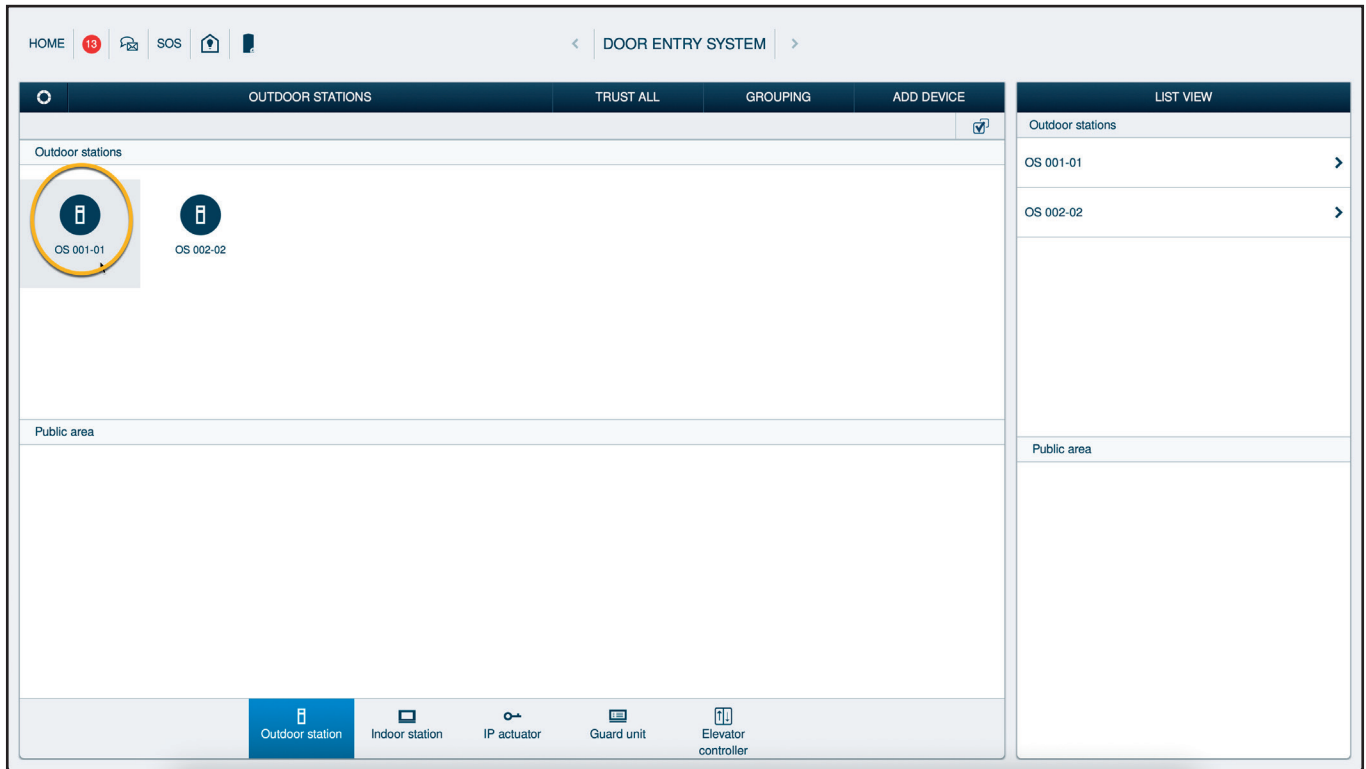
When signed-in successfully, the first menu shown is the Main Menu.

- Click on the Door Entry System button.



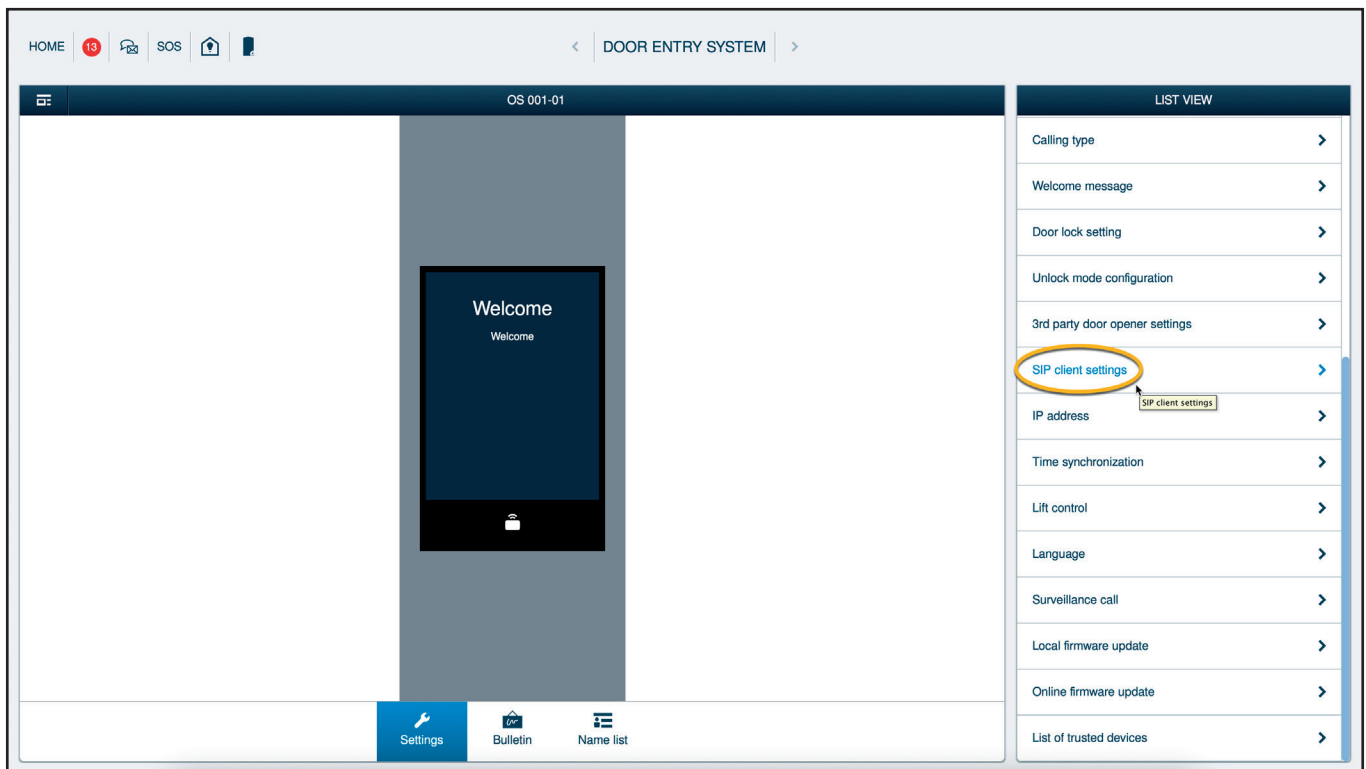
Smart Access Point Pro - Main screen

- The Door Entry System screen will show. Select the Outdoor Station to configure



Smart Access Point Pro - Door Entry System - Select Outdoor Station

- Click on the SIP client settings to open the SIP settings of the Outdoor Station



Smart Access Point Pro - Door Entry System - Open SIP client settings

- For communication over TCP, provide / change the following information:

| Advanced Settings | |
|--------------------|--|
| Advanced settings | Enable the Advanced settings |
| Device ID & number | |
| Call number | Use the Username provided by the CyberGate Management Portal |
| Domain | cybergate.cybertwice.com |
| Display name | Use the Username provided by the CyberGate Management Portal |
| SIP account | |
| Username | Use the Username provided by the CyberGate Management Portal |
| Password | Use the Password provided by the CyberGate Management Portal |
| SIP server | |
| IP address | cybergate.cybertwice.com |
| Port | For TCP communication, use 5060 |
| SIP protocol | |
| SIP protocol | Select TCP |
| Transport protocol | |
| Transport protocol | Select RTP |

- Click 'Save' button when done.

The screenshot displays the configuration interface for the Door Entry System. The main display area shows a 'Welcome' message. The right sidebar contains the following configuration settings:

- Advanced settings:** Advanced settings
- Status Of registration:** **C** Registered successfully
- Device ID & number:**
 - Call Number: KFBWB1ED3HNV
 - Domain: cybergate.cybertwice.com
 - Display Name: KFBWB1ED3HNV
- SIP account:**
 - User name: KFBWB1ED3HNV
 - Password: [Redacted]
- SIP server:**
 - IP address: cybergate.cybertwice.com
 - Port: 5060
- SIP protocol:**
 - UDP
 - TCP
 - TLS
- Transport protocol:**
 - sRTP
 - RTP

A 'Save' button is visible at the bottom right of the configuration panel.

Smart Access Point Pro - Door Entry System - SIP settings TCP

- For secure communication over TLS, provide / change the following information:

| SIP server | |
|--------------------|-------------|
| Port | Use 5061 |
| SIP protocol | |
| SIP protocol | Select TLS |
| Transport protocol | |
| Transport protocol | Select sRTP |

The screenshot displays the configuration interface for a Smart Access Point Pro, specifically for the Door Entry System. The main screen shows a 'Welcome' message on a mobile device. The right-hand panel, titled 'LIST VIEW', contains the SIP settings for TLS. The settings are as follows:

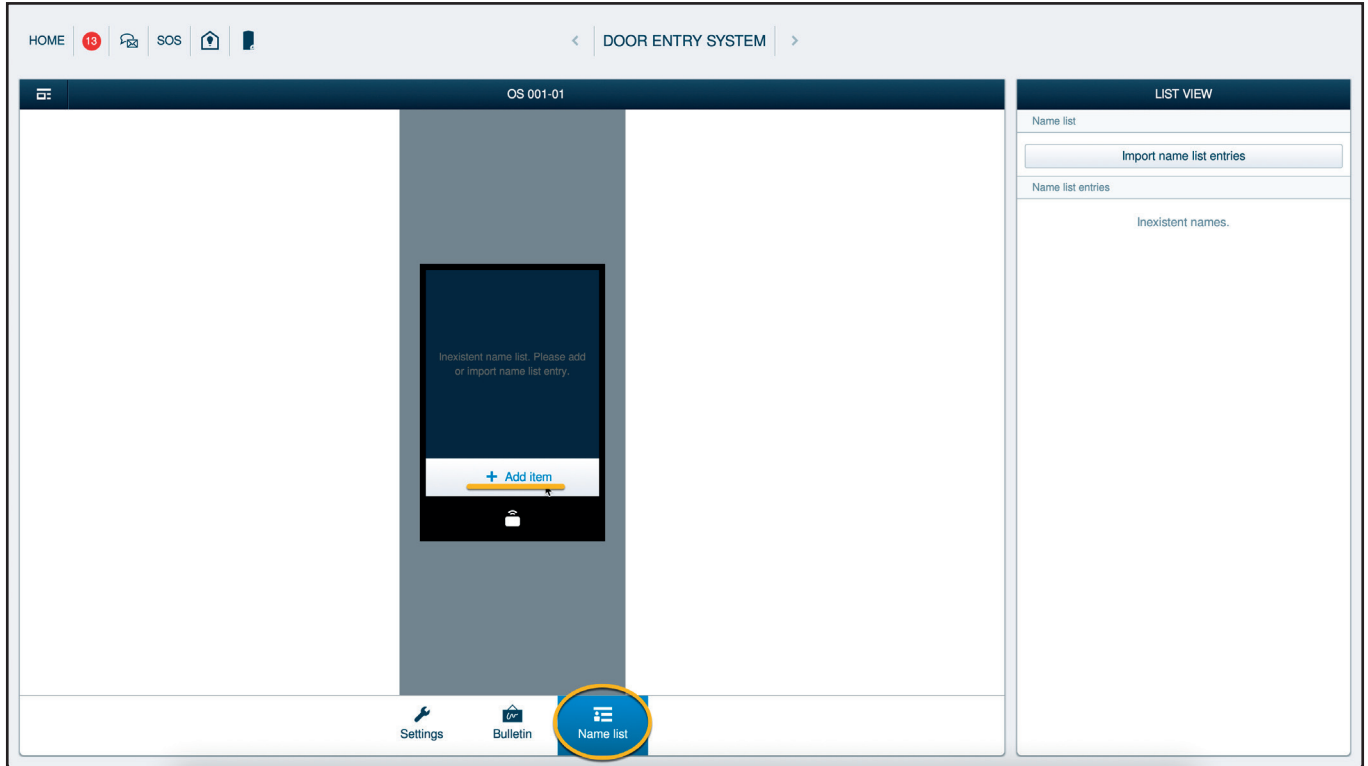
- Advanced settings:** Advanced settings
- Status Of registration:** **C** ● Registered successfully
- Device ID & number:** OS 001-01
- Call Number:** KFBWB1ED3HNV
- Domain:** cybergate.cybertwice.com
- Display Name:** KFBWB1ED3HNV
- SIP account:**
 - User name:** KFBWB1ED3HNV
 - Password:** [Redacted]
- SIP server:**
 - IP address:** cybergate.cybertwice.com
 - Port:** 5061
 - SIP protocol:** TLS (selected), UDP, TCP
 - Transport protocol:** sRTP (selected), RTP

At the bottom of the right panel, there is a 'Save' button with a checkmark icon.

Smart Access Point Pro - Door Entry System - SIP settings TLS

Add a call destination for the Ourdoor Station.

- Click on Name list
- Click on the '+ Add item' to add a destination to call



Smart Access Point Pro - Door Entry System - Name list - Add name

- Provide / change the following information:

| Type | |
|------------------------|---|
| Type | Select SIP |
| SIP number | |
| SIP number | Teams user name without the domain name * |
| Resedent(s)/Tenant(s) | |
| Last name/Company name | Last name of the destination to dial |
| First name | First name of the destination to dial |

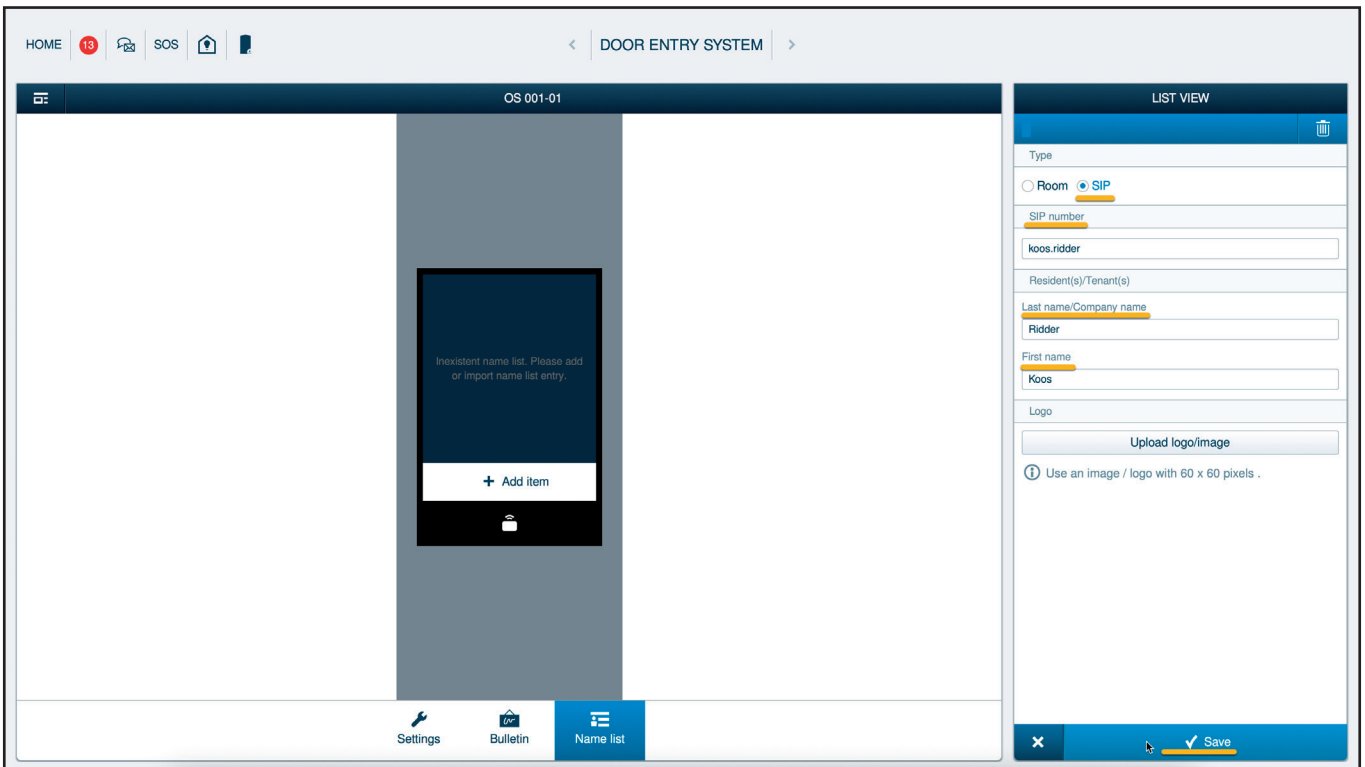
* For example, the user 'Koos Ridder, with the Teams name:

koos.ridder@mycompany.com

will translate to this destination address:

koos.ridder

- Click the 'Save' button when done.



Smart Access Point Pro - Door Entry System - Name list - Added name

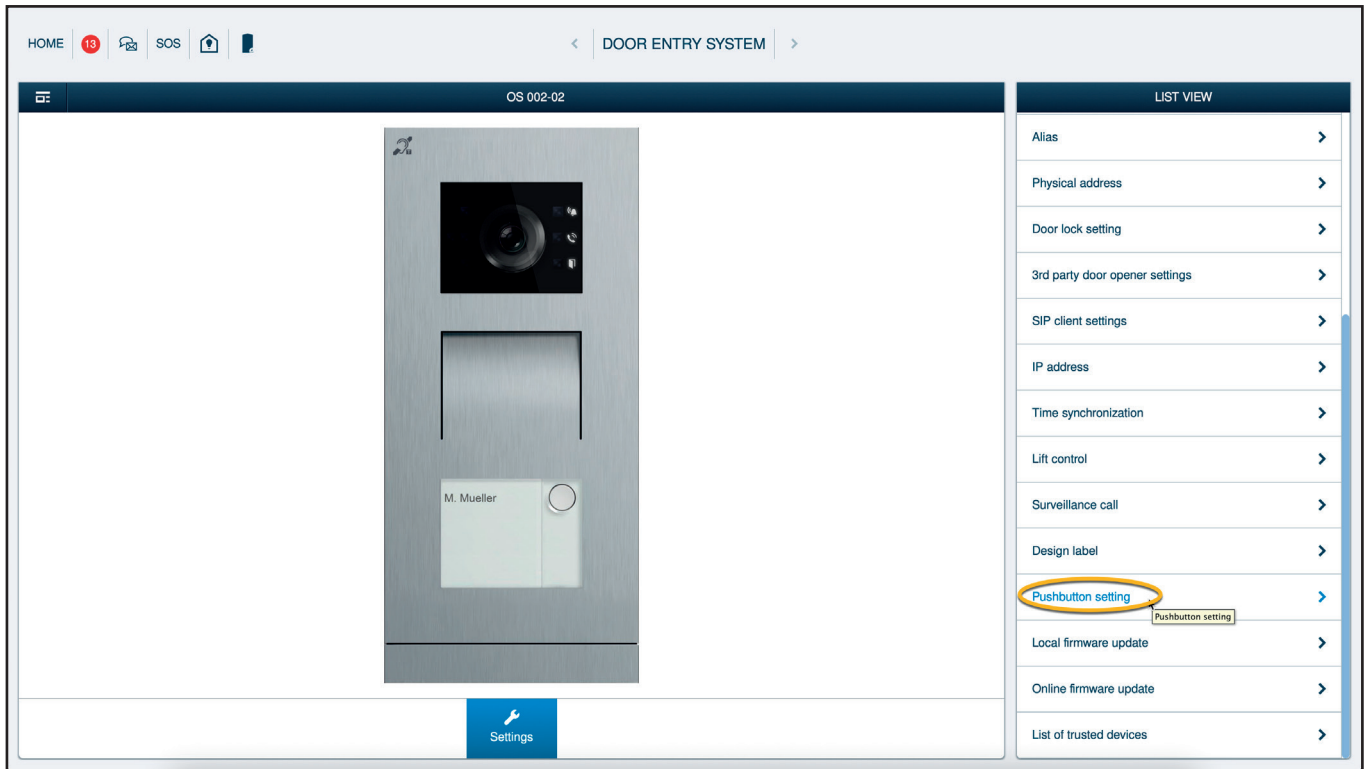
After successful adding of the call destination, the destination will be shown on the display of the Outdoor Station.

The screenshot displays the configuration interface for a Door Entry System. The top navigation bar includes 'HOME', 'SOS', and 'DOOR ENTRY SYSTEM'. The main content area is titled 'OS 001-01' and features a central preview of a mobile device. The mobile device screen shows a name list entry: 'Ridder, Koos # 147 Floor 0' with a yellow bar and an '+ Add item' button. To the right, the 'LIST VIEW' sidebar contains a search bar and a list of entries, with 'Ridder, Koos' selected and highlighted in yellow. The bottom navigation bar includes 'Settings', 'Bulletin', and 'Name list'.

Smart Access Point Pro - Door Entry System - Name list - Name added successfully

The configuration of an Outdoor Station with buttons instead of a display, follow the next steps to configure the call destination.

- Click on the Pushbutton setting



Smart Access Point Pro - Door Entry System - Name list - Pushbutton setting

- Provide / change the following information:

Pushbutton setting

| | |
|---|--|
| 1 | Teams user name without the domain name, starting with an 'S'* |
|---|--|

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

koos.ridder@mycompany.com

will translate to this destination address:

S:koos.ridder

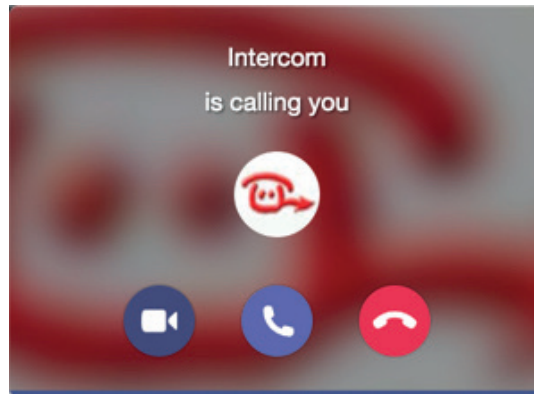
- Click the 'Save' button when done.

The screenshot shows the configuration interface for a Smart Access Point Pro. The main area displays a door entry system with a camera and a display showing 'M. Mueller'. The right sidebar is titled 'LIST VIEW' and shows the 'Pushbutton setting' configuration. The setting is for ID '1' and is set to 'S : koos.ridder'. A legend explains the letters: G = call to group, R = call to room, GU = call to guard unit, L = light switch, please select the corresponding IPA, S = call sip. A 'Save' button is visible at the bottom right of the sidebar.

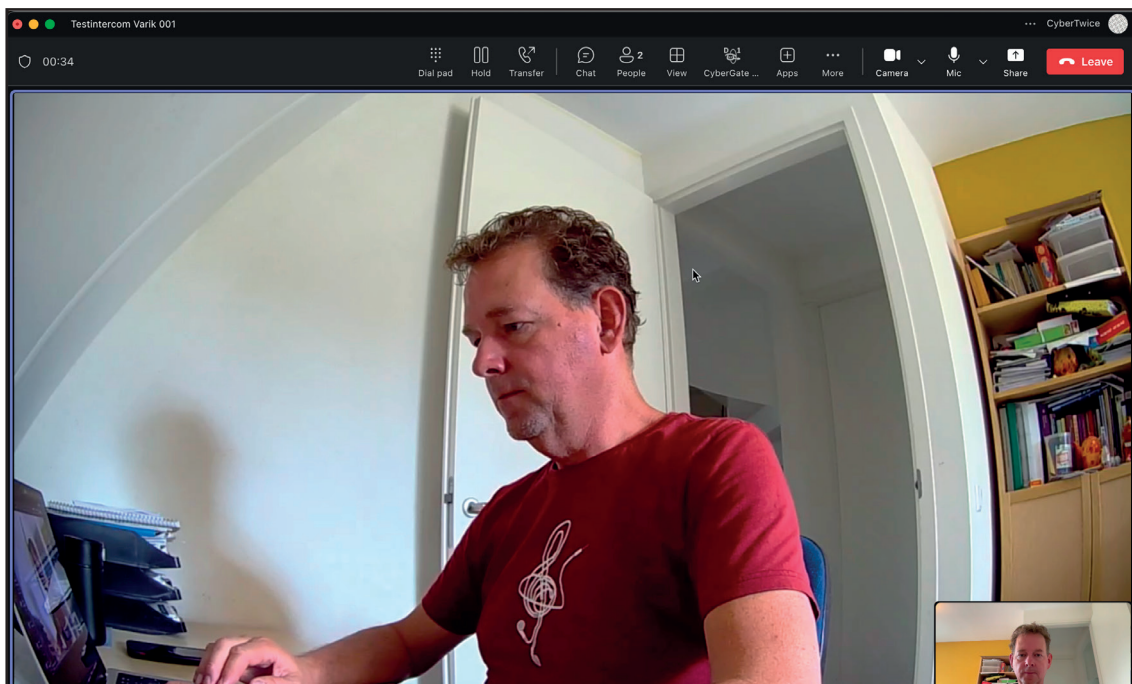
Smart Access Point Pro - Door Entry System - Name list - Pushbutton setting - Name added

Configuration is now done. Press on the name of the destination on the Outdoor Station (or on the pushbutton) to initiate a call to the configured Teams User.

If configured correctly, the Teams client will notify you of an incoming call. Answer it by clicking the camera symbol.



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



To open the door from the Teams call, click on Dial pad symbol. Use the code configured followed by a # (the default code for the Outdoor Station is '1' so '1#'), this will trigger the relay in the Outdoor Station 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 describes the installation of the app and all three features in detail.

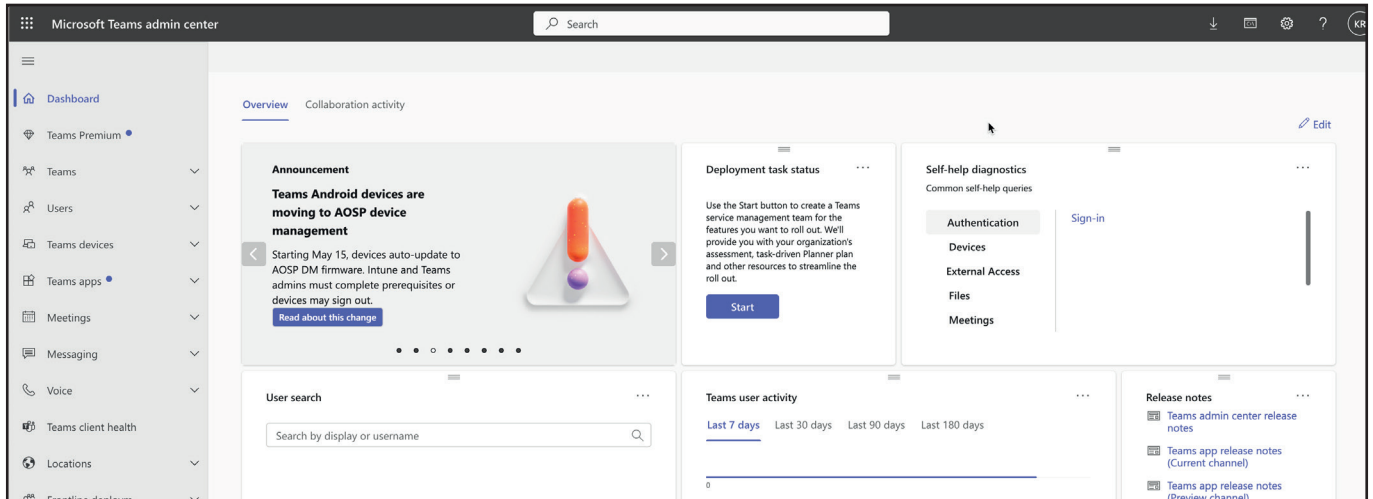
The installation of the CyberGate app for Microsoft Teams as described in this document makes the CyberGate app available for every user in the organisation. Of course this can be modified by selecting different user groups and / or setup policies to match the policies of your organisation.



Installation

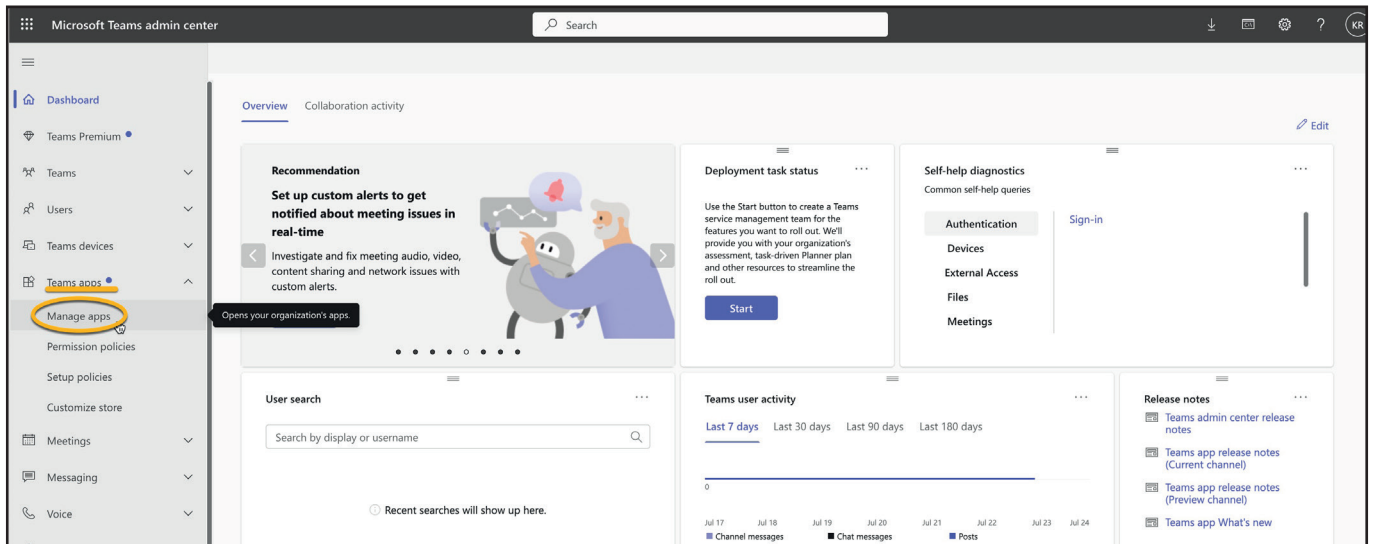
How to install

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



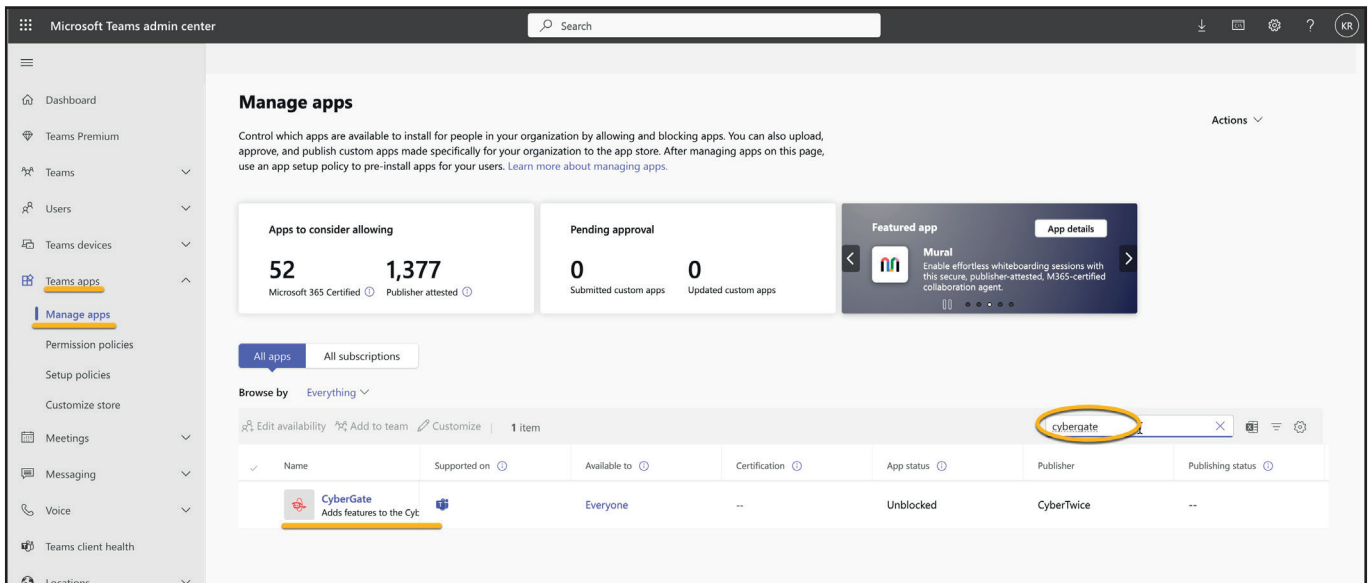
Microsoft Teams Admin Portal - Dashboard

- Navigate to the menu Teams apps - Manage apps



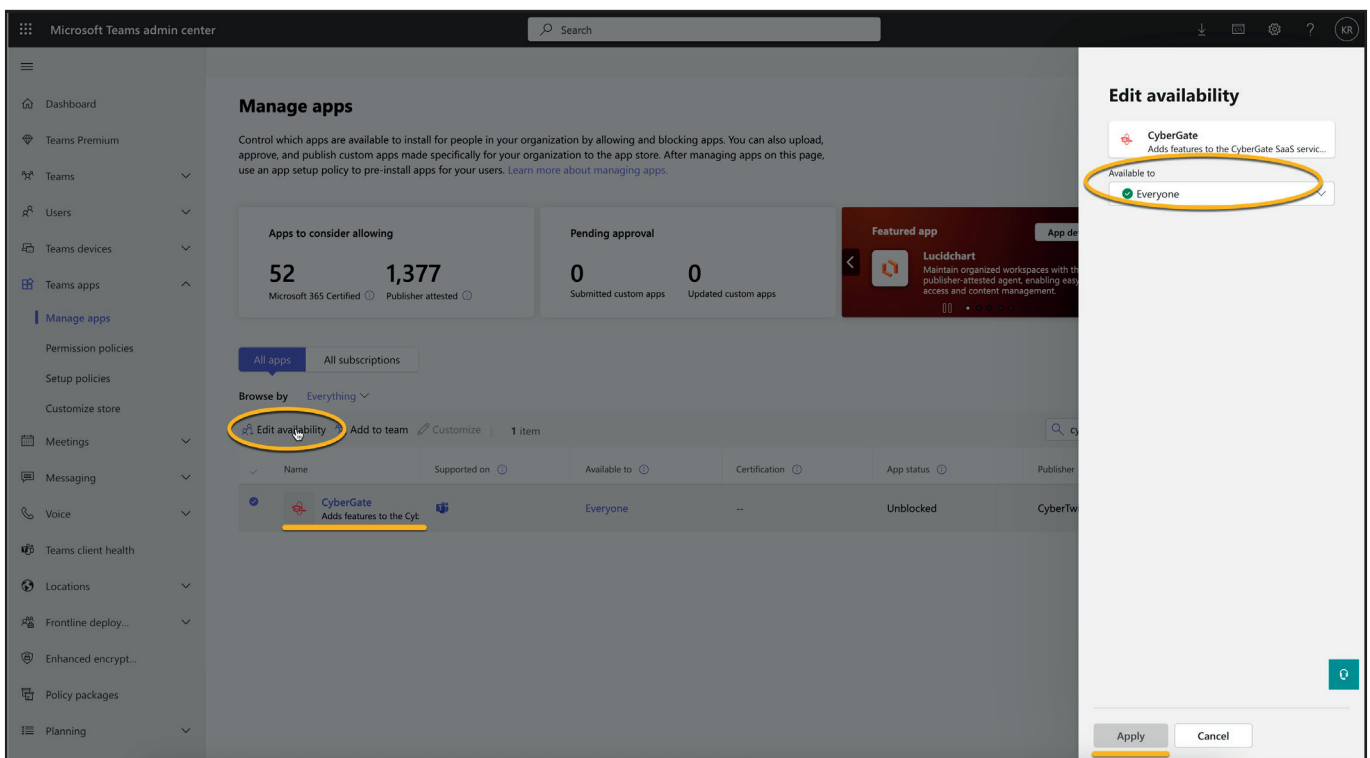
Microsoft Teams Admin Portal - Teams apps - Manage apps

- 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

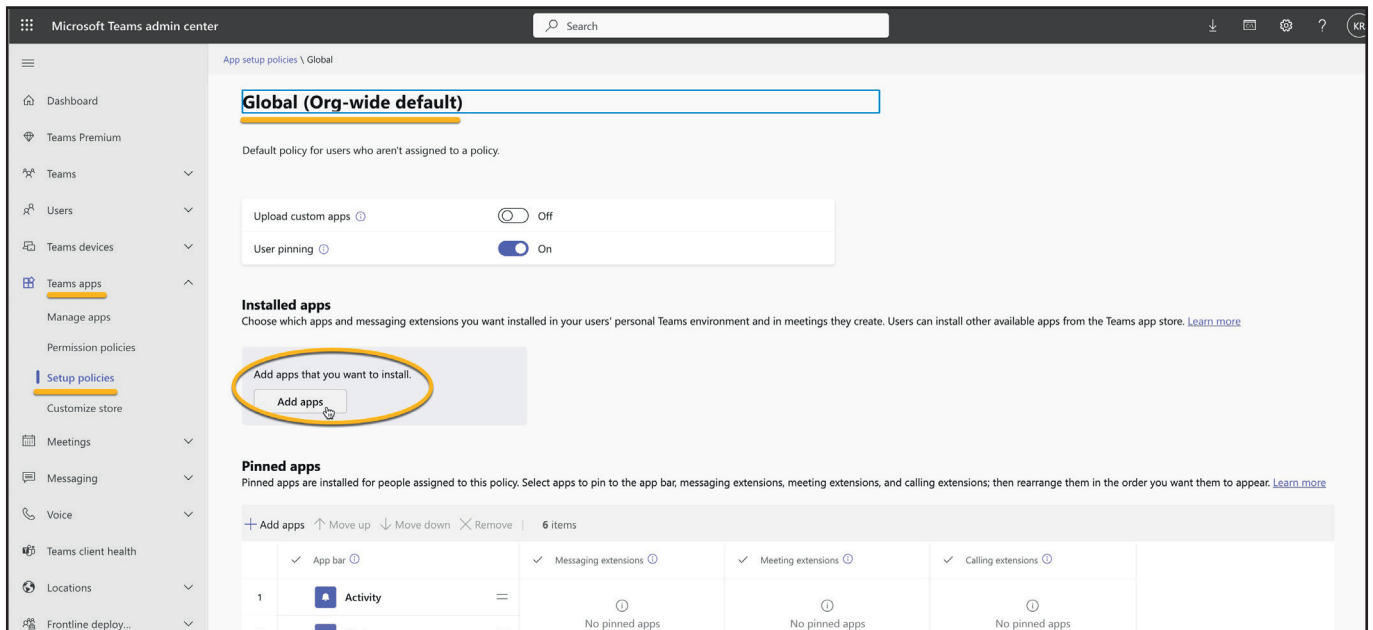
- Select the policy 'Global (Org-wide default)'

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 structure is as follows:

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

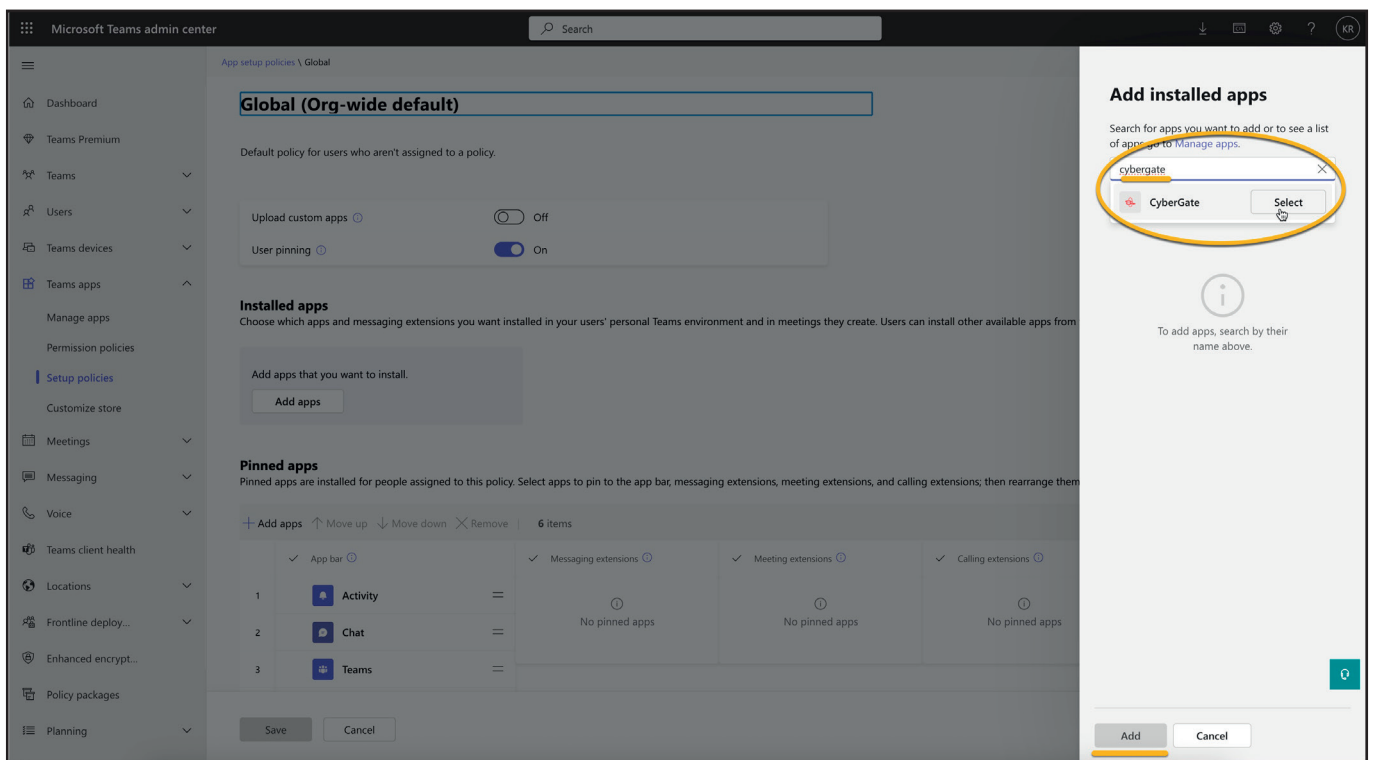
Microsoft Teams Admin Portal - Teams apps - Setup policies - Select 'Global'

- 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.

Microsoft Teams admin center

App setup policies \ Global

Global (Org-wide default)

Default policy for users who aren't assigned to a policy.

Upload custom apps Off

User pinning On

Installed apps
Choose which apps and messaging extensions you want installed in your users' personal Teams environment and in meetings they create. Users can install other available apps from the Teams app store. [Learn more](#)

+ Add apps × Remove | 1 item

| ✓ | Name | App ID | Publisher |
|-------------------------------------|-----------|--------------------------------------|------------|
| <input checked="" type="checkbox"/> | CyberGate | 8dd84f10-2fbf-4c8b-9116-7eb326bd7c8e | CyberTwice |

Pinned apps
Pinned apps are installed for people assigned to this policy. Select apps to pin to the app bar, messaging extensions, meeting extensions, and calling extensions; then rearrange them in the order you want them to appear. [Learn more](#)

+ Add apps ↑ Move up ↓ Move down × Remove | 6 items

| ✓ | 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 |

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 center

Upload custom apps Off

User pinning On

Installed apps
Choose which apps and messaging extensions you want installed in your users' personal Teams environment and in meetings they create. Users can install other available apps from the Teams app store. [Learn more](#)

+ Add apps × Remove | 1 item selected

| ✓ | Name | App ID | Publisher |
|-------------------------------------|-----------|--------------------------------------|------------|
| <input checked="" type="checkbox"/> | CyberGate | 8dd84f10-2fbf-4c8b-9116-7eb326bd7c8e | CyberTwice |

Pinned apps
Pinned apps are installed for people assigned to this policy. Select apps to pin to the app bar, messaging extensions, meeting extensions, and calling extensions; then rearrange them in the order you want them to appear. [Learn more](#)

+ Add apps ↑ Move up ↓ Move down × Remove | 6 items

| ✓ | 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 | | | | | | |
| 4 | Calendar | | | | | | |
| 5 | Calling | | | | | | |
| 6 | OneDrive | | | | | | |

Save Cancel

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

Note: If you already have an earlier version of the CyberGate app pinned, please remove this pinned version first before pinning the new CyberGate app! Not doing so will result in a non-working CyberGate app.



- 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 "Add pinned apps" and contains a search box with "cybergate" entered. Below the search box, a list of search results is displayed, with "CyberGate" selected. The "Select" button next to "CyberGate" is highlighted with a yellow circle. The background shows the "Pinned apps" section of the admin portal, which lists various apps like Activity, Chat, Teams, Calendar, Calling, and OneDrive. The "Add" button at the bottom right of the "Add pinned apps" panel is also highlighted with a yellow bar.

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 CyberGate pinned to the App bar, Calling extensions, and Meeting extensions.

| 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

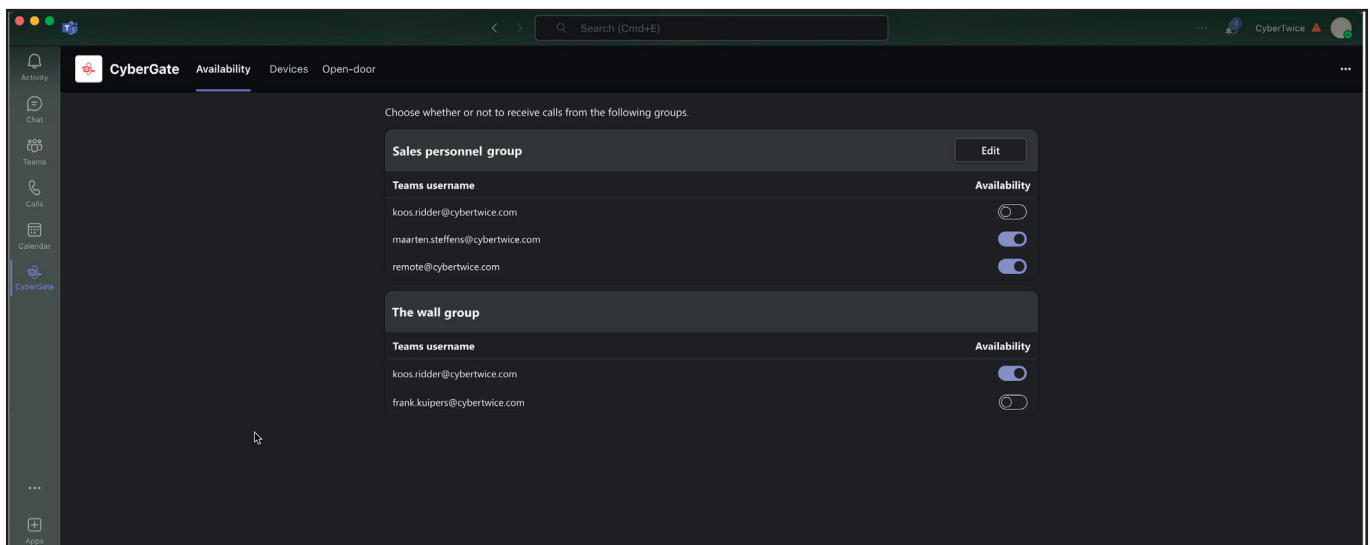
The 'Sale personnel group' contains three users and the 'The wall group' contains two users.

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).

Devices

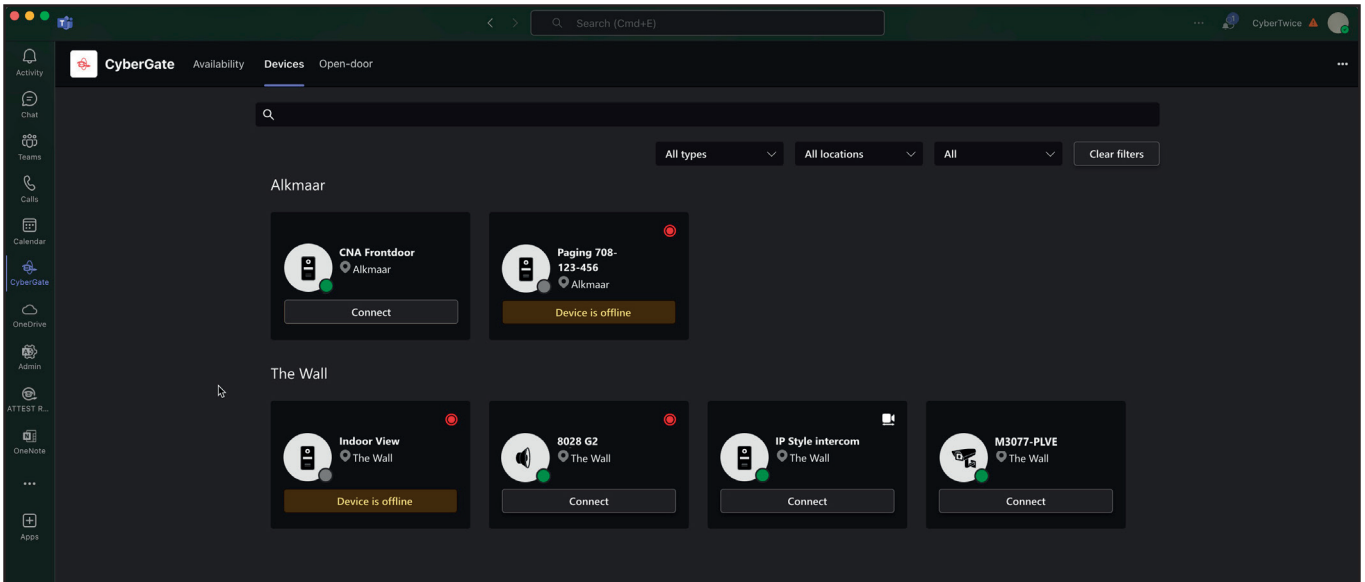
How to use

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 easialy 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 Kees Ridder
fr. in.onmicrosoft.com

ADMINISTRATION

- Licensing

BASIC

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

CAMERA

- Meeting

TEAMS APP

- Availibility
- 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 | QV9ZTCASCUSHH0A5CHF8 | AZZ ●●●●●●●● | yes | no | yes | Add Remove |

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 *#).

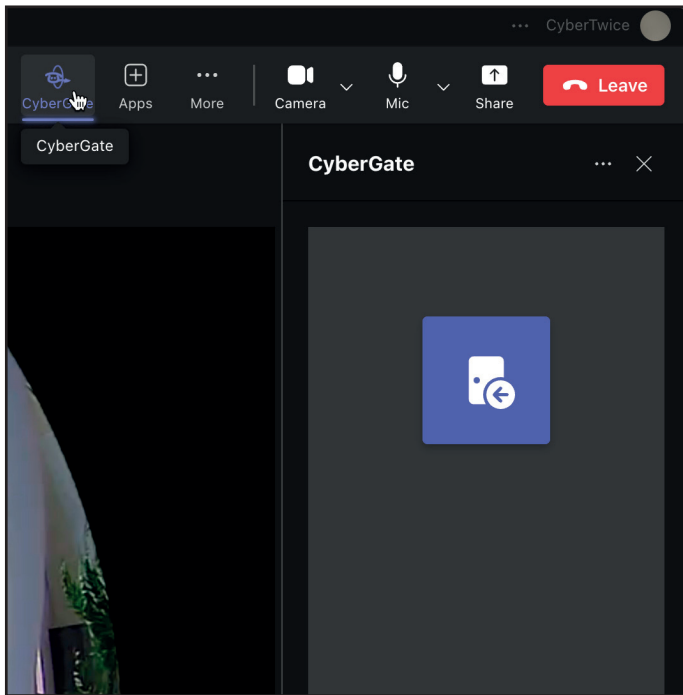
Detected SIP username
MONET

[Cancel] [Update]

CyberGate Management Portal - Device details

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 | 29-07-2025 | KR | Initial version |