

TechNote: CyberGate

Version: 1.5.1 ENG
Date: 17-11-2025



**Connect a SIP Intercom / Pager /
Camera to Teams using CyberGate**

Table of Contents

| | |
|--|-----------|
| Introduction | 3 |
| About this manual | 4 |
| Workflow summary to purchase, activate and configure CyberGate | 5 |
| Prerequisites | 6 |
| Step 1: Purchase of CyberGate | 7 |
| Purchase in Microsoft Marketplace | 7 |
| Purchase in Microsoft Azure | 14 |
| Step 2: Configure CyberGate in the Management portal | 19 |
| Step 3: Configure the device | 24 |
| Appendix A: How to use the CyberGate Management Portal | 25 |
| Administration | 26 |
| Licensing | 26 |
| Basic | 27 |
| Global | 27 |
| Network | 29 |
| Portal access | 30 |
| Device | 32 |
| Multi-ring | 35 |
| SIP trunk settings | 37 |
| Camera | 38 |
| Meeting | 38 |
| Teams App | 40 |
| Availability | 41 |
| Device | 42 |
| Appendix B: Configure the display name of the device | 44 |
| Appendix C: Call recording | 50 |
| Steps to follow to enable recording in CyberGate | 51 |
| Activation of the recording feature | 52 |
| Search and replay recorded calls | 55 |
| Modify the recording related settings | 59 |
| Appendix D: Network requirements | 64 |
| Outbound port configuration | 64 |
| SIP ALG | 64 |
| Communication Test Script | 65 |
| Document History | 66 |

Introduction

With CyberGate you can connect a SIP audio- or video intercom, a SIP pager or SIP camera to your Microsoft Teams environment.

Teams users can answer incoming calls or initiate outgoing calls with 2-way audio and live video on a Teams desktop client, Teams desk phone and the Teams smartphone app and control relay switches on the devices (eg. to open a door or a gate).

About this manual

This manual describes the procedure how to purchase and configure CyberGate. Follow the three steps to get CyberGate up and running in the default configuration. Follow the appendices for detailed configuration, setup and functionalities:

- **Appendix A: How to use the CyberGate Management Portal.** Configure CyberGate for your Teams Tenant, manage subscriptions and connected Devices.
- **Appendix B: Configure the display name of the device.** Assign a Display Name to your connected Devices in CyberGate. The display name is the name of the device that is shown in Microsoft Teams.
- **Appendix C: Call Recording.** An optional and complementary feature to record audio & video communications from / to your connected Devices.
- **Appendix D: Network requirements.** A summarisation of the required network settings and troubleshooting suggestions.

Note:

The configuration of the intercom, pager, speaker, camera or amplifier is not described in this manual as each compatible device has its own manual. The device configuration manuals can be found on the CyberTwice support website: <https://support.cybertwice.com>



Workflow summary to purchase, activate and configure CyberGate

“Step 1: Purchase of CyberGate” on page 7

Describes the procedure how to purchase CyberGate at Microsoft AppSource or Microsoft Azure Marketplace

“Step 2: Configure CyberGate in the Management portal” on page 19

Setup CyberGate and the connected Devices

“Step 3: Configure the device” on page 24

All compatible CyberGate brands and links to the installation instructions that are needed to configure the device for use with CyberGate

Ready to use!

Prerequisites

To be able to purchase and use CyberGate, the following prerequisites apply:

- Microsoft Office 365 Business subscription with Teams
- A device (IP Intercom, IP Pager, IP Camera) compatible with CyberGate (compatible devices: [Link](#))

Start with the purchase of CyberGate in Microsoft Marketplace. Microsoft Marketplace is the main store for software purchases hosted by Microsoft.

Note:

Log in to Microsoft Marketplace with **global administrator privileges** of your organization!

At the end of the purchase & activation process, you will be redirected to the CyberGate Management Portal where you must activate your CyberGate subscription. Please use the same user with **global administrator privileges** as used to purchase CyberGate for this activation step.



Step 1: Purchase of CyberGate

Follow the instructions below to purchase CyberGate in Microsoft Marketplace.

Already purchased? Skip to “Step 2: Configure CyberGate in the Management portal” on page 19

Purchase in Microsoft Marketplace

- Click on the following link to go to Microsoft Marketplace: <https://marketplace.microsoft.com>
- Search for ‘cybergate’. You’ll find multiple CyberGate results. Depending of the device type your connecting, choose between:
 - CyberGate for IP Video Intercoms with Teams
 - CyberGate for IP Cameras with Teams
 - CyberGate for IP Paging with Teams

The screenshot shows the Microsoft Marketplace interface with search results for 'cybergate'. The search results are displayed in a grid format. The first row contains five results, and the second row contains two results. Each result card includes the product name, publisher (CyberTwice B.V.), a brief description, a rating, and a 'Get it now' or 'Free trial' button.

| Product Name | Rating | Price / Trial |
|---|------------------|-------------------------------------|
| CyberGate | 3.7 (57 ratings) | Additional purchase may be required |
| CyberGate for IP Video Intercoms with Teams | 4.8 (5 ratings) | Starts at € 23,94434/user/1-month |
| CyberGate for IP Paging with Teams | | Starts at € 23,04743/user/1-month |
| CyberGate for IP Cameras with Teams | | Starts at € 23,04743/user/1-month |
| CyberGate Add-on: Audio Improvement by... | | Starts at € 2,80779/user/1-month |
| ATTEST for Teams | | Starts at € 9,30994/1-month |
| Attest Replay | 4.0 (1 ratings) | Free |

Marketplace and the search result for ‘cybergate’

- Click on ‘Free trial’ to start the purchasing procedure

The overview page provides information regarding CyberGate, plans, pricing information and reviews.

- Click 'Get it now' to start the purchasing procedure

Microsoft | Marketplace

Products Search Marketplace

All Products Categories Industries Partners

Products CyberGate for IP Video Intercoms with Teams

CyberGate for IP Video Intercoms with Teams
by CyberTwice B.V.

SaaS

Free trial Azure benefit eligible

★ 4.8 (5 ratings)

Starting at € 23,94434/user/1-month **Get it now** Save to my list

Overview Plans + Pricing Ratings + reviews Details + support

Connect your IP Video Door Intercom to Microsoft Teams

Is your organization migrating from a traditional SIP based phone system to Microsoft Teams and you want to connect your existing **SIP Video Door Intercom** to Teams?

CyberGate SaaS hosted in Azure makes this migration painless and provides **two-way audio** and **live video** to the receiving user. Teams users answer incoming calls from the video door station on their Teams desktop client, Teams compatible desk phone or Teams Mobile app and could open the door for visitors.

Features

- CyberGate is published on Microsoft AppSource and Azure Marketplace for online purchase and activation and works for Teams users with a M365 Business or Enterprise license.
- With CyberGate there is no need for: an SBC, direct routing, phone system, operator connect or additional Teams licenses.
- Two-way audio and live video from your (existing) SIP video intercom to the Teams user's desktop client, Teams compatible desk phone and Teams mobile app.
- Remotely open a door or gate using the dedicated 'Open the door button' in Teams.
- Call individual Teams users or configure group names to call multiple users simultaneously.
- Optional Call Recording feature providing audio and video recording.
- More devices to connect to Teams? Link your IP Pager, IP Visual Alerter or IP Amplifier to Teams for PA announcements or pre-recorded audio messages or your IP Camera.

Pricing

CyberGate subscription fees are device based, in a monthly- or annual plan, independent of the number of Teams users.

- Video Door Intercom: 1 (one) subscription *per intercom device*

Check the CyberGate [compatibility sheet](#), or [contact us](#) for any questions.

At a glance

The images in the 'At a glance' section show a person using a Teams client, a diagram of the CyberGate architecture, and screenshots of the Teams interface displaying video intercom feeds.

CyberGate 'Overview'

- Select the CyberGate flex plan and click 'Next'

Microsoft | Marketplace

Products Search Marketplace

All Products Categories Industries Partners

Apps > CyberGate for IP Video Intercoms with Teams > Checkout

Checkout

Plan Price + billing Payment Complete purchase

Select a plan

CyberGate for IP Video Intercoms with Teams

Please note some prices will be changing. View details below.

CyberGate flex plan Free trial

Description

Connect your IP Video Door Intercom to Microsoft Teams with two-way audio and live video to the Teams desktop client. Teams desk phone and Teams Smartphone app and open the door remotely. CyberGate needs no extra hardware and works without SBCs or MS Phone System.

CyberGate subscription fees are per IP INTERCOM DEVICE, INDEPENDENT OF THE NUMBER OF TEAMS USERS in your organization. IP Video Door Intercom: 1 CyberGate subscription per Intercom DEVICE Monthly or Annual Billing Term 1-month free trial period included

Check the CyberGate compatibility sheet, or contact us for any questions.

Number of users 1-1,000,000

Price/payment options

1-month subscription

- First month free, then € 23,94434/user/1-month

1-year subscription

- First month free, then € 248,48737/user/1-year
- ⓘ Upcoming price change

2-year subscription

- First month free, then € 242,62629/user/year

3-year subscription

- First month free, then € 235,21785/user/year

Next Have an Azure subscription? Get the offer in the Azure Portal. The purchase can also contribute towards your organization's Azure commitment. [Learn more](#)

CyberGate 'Plan'

- Select the billing term.
- For pricing check the CyberGate pricing page ([Link](#))

Note:

All CyberGate Billing Terms come with a 30 day free trial period.

You can have one subscription to CyberGate and use multiple devices with that subscription. The 'Number of Users' can be read as the 'number of devices' used with this subscription. You can always modify the amount of devices on this subscription later on in the CyberGate Management portal.

- Make sure that 'Auto-renew' is 'On' (the 1st month is a free trial period, and subscriptions auto renew until cancelled).
- Select the 'Number of Users' (read: number of devices)
- If your Tenant has an Azure subscription, you'll be offered the option to purchase CyberGate in Azure. Payment will be handled through the Azure subscription.

Note:

Payment via Azure? "Purchase in Microsoft Azure" on page 14 for instructions how to continue purchase CyberGate

- When done, click 'Next'

The screenshot shows the Microsoft Marketplace checkout page for 'CyberGate for IP Video Intercoms with Teams'. The page is titled 'Checkout' and has a navigation menu on the left with options: Plan, Price + billing (selected), Payment, and Complete purchase. The main content area is divided into sections:

- Price + billing:** Includes a warning: 'Please note some prices will be changing. View details below.'
- Billing term:** Options include 1-month subscription (selected), 1-year subscription, 2-year subscription, and 3-year subscription.
- Price/payment options:** 'First month free, then € 23,94434/user/1-month'.
- Auto-renew:** A toggle switch is set to 'On'.
- Number of users:** A dropdown menu is set to '1'.

Below the pricing section, there are three payment method options:

- Credit card:** 'Use a credit card to make an online payment. Accepted payment methods: VISA, Mastercard, American Express.'
- Invoice pay New!:** 'If your organization has been approved for payment by invoice, select Invoice pay on the next page to pay with a check or wire transfer. Learn more about paying by invoice.'
- Azure subscription:** 'Use your Azure subscription to purchase this app and benefit your organization by reducing your existing Azure commitment. Learn more. Get it in Azure portal.'

CyberGate price + billing

- Review the details (address & payment method). You can also add a new payment method if no payment method is available.

Microsoft | Marketplace

Products Search Marketplace

All Products Categories Industries Partners

Apps > CyberGate for IP Video Intercoms with Teams > Checkout

Checkout

- Plan
- Price + billing
- Payment
- Complete purchase

| Product name | Price (EUR) | Quantity | Subtotal (EUR) |
|--|---|----------|---------------------|
| Offer: CyberGate for IP Video Intercoms with Teams | First month free, then € 23,94434/user/one-time payment | 1 | € 23,94 for 1 month |
| Plan: CyberGate flex plan Free trial | | | |
| Billing term: 1-month subscription | | | |
| Auto-renew: On | | | |

Sold to address *
Enter the address of the legal entity responsible for payment and identified on the invoice. The address provided here is used to determine your tax rate.

Billing account
Infringement
[Edit](#)
NL

Bill to *
Select the billing profile you want to use for this purchase. You can also edit an existing profile. [Learn more about billing profiles](#)

Billing profile
Demo billing profile - visa *
[Edit](#) [Add new](#)

Tax ID [Add a tax ID](#)

Summary

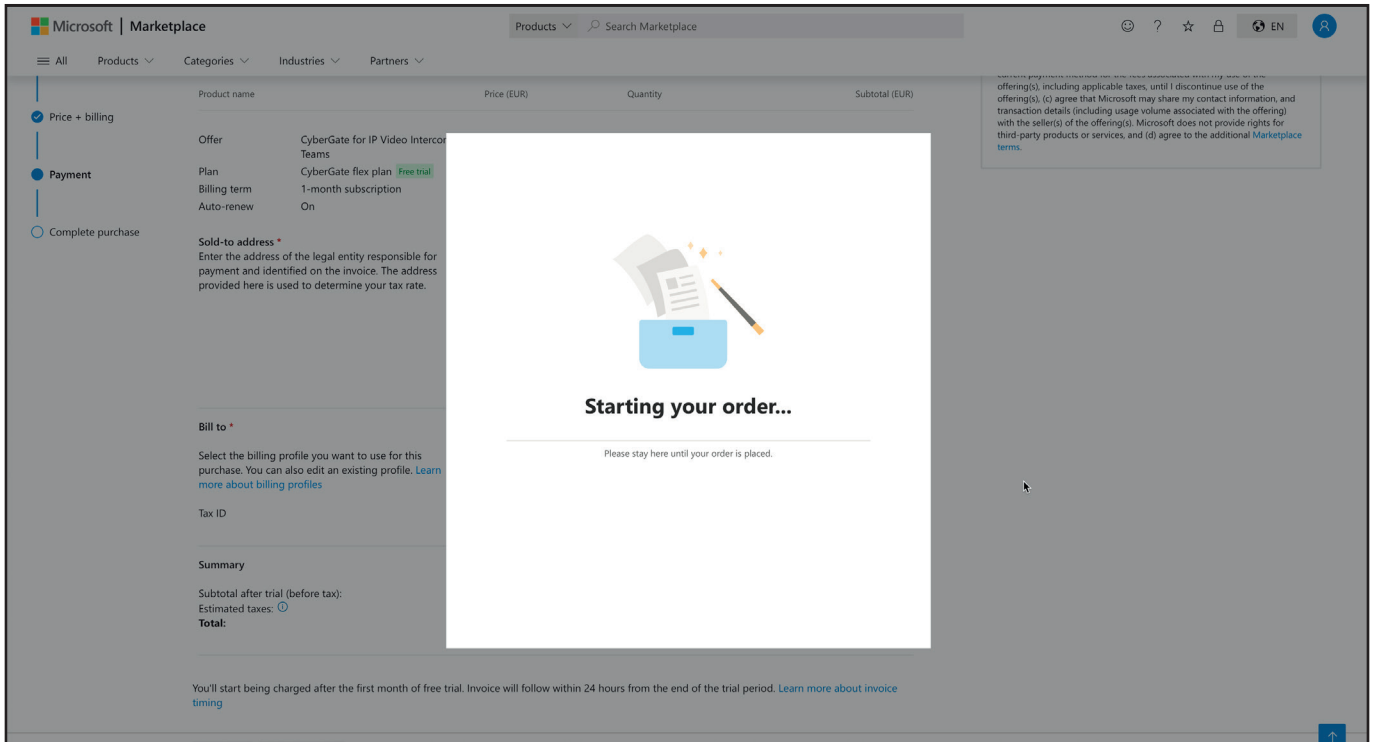
| | |
|------------------------------------|---------|
| Subtotal after trial (before tax): | € 23,94 |
| Estimated taxes: | € 0,00 |
| Total: | € 0,00 |

You'll start being charged after the first month of free trial. Invoice will follow within 24 hours from the end of the trial period. [Learn more about invoice timing](#)

[Back](#) [Accept agreement & place order](#)

CyberGate complete purchase

- When done, click 'Accept agreement & place order'.

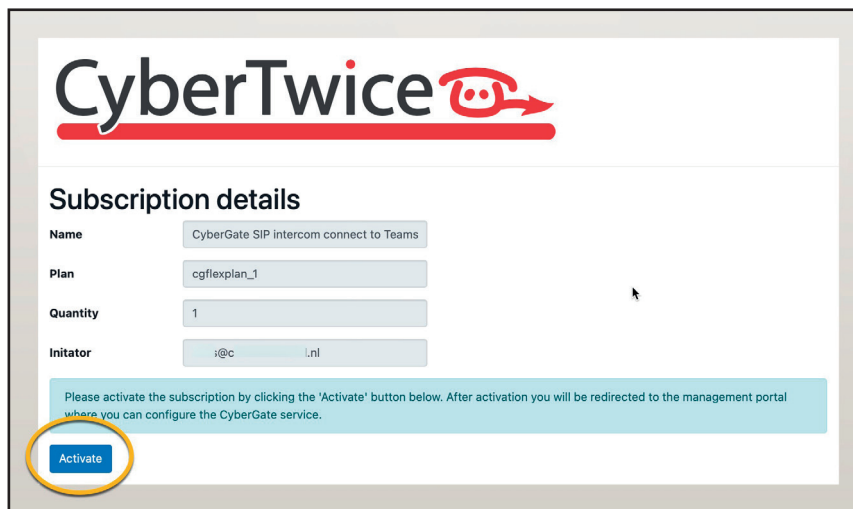


CyberGate purchasing in progress

The Microsoft Marketplace will redirect you to the CyberGate Management Portal where you can activate your CyberGate Purchase.

Note:
 Log in with a user with **global administrator privileges** of your organization, this is mandatory to activate CyberGate. !

- Click 'Activate' to activate your CyberGate subscription. It will take you to the dashboard of the admin portal.



CyberGate overview of the 'Subscription details'

CyberTwice

Subscription details

Name: CyberGate SIP intercom connect to Teams

Plan: cgflexplan_1

Quantity: 1

Initiator: l...s@c...n.onmicrosoft.com

Please activate the subscription by clicking the 'Activate' button below. After activation you will be redirected to the management portal where you can configure the CyberGate service.

Activate **Subscription successfully activated!**

CyberGate successfully activated

The CyberGate Management Portal will open and show the License overview.

CyberTwice Koos Ridder
fr...n.onmicrosoft.com

License overview

| Name | Created | Quantity | Enabled |
|-------------------------------------|------------|----------|---------|
| fr...n.onmicrosoft.com subscription | 2024-08-06 | 1 | yes |

CyberGate Management Portal License overview

Continue with “Step 2: Configure CyberGate in the Management portal” on page 19.

Purchase in Microsoft Azure

Continuation from page 10

In Azure, the CyberGate offer will be opened automatically.

- Select a Resource group for your CyberGate purchase or create a new Resource group
- Name the CyberGate subscription
- Select the billing term and payment method.
- For pricing check the CyberGate pricing page ([Link](#))

Note:

All CyberGate Billing Terms come with a 30 day free trial period.



You can have one subscription to CyberGate and use multiple devices on that subscription. The 'User count' can be read as the 'number of devices' used with this subscription. You can always modify the amount of devices on this subscription later on, in the CyberGate Management portal.

- Select the number of users
- Make sure that 'Recurring billing is 'On' (the 1st month is a free trial period, and subscriptions auto renew until cancelled).
- When finished, click 'Review + Subscribe'.

Microsoft Azure

Home > CyberGate SIP intercom connect to Teams >

Subscribe To CyberGate SIP intercom connect to Teams

Subscribe to plan

* Basics Tags Review + subscribe

Fill out the plan details. After you've finished subscribing, configure your SaaS account on the publisher's website to complete the process.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Resource group location *

SaaS details

Name *

Plan

CyberGate flex plan - 1-month

With the CyberGate per month or per year subscription you can connect a SIP H264 video door intercom to Microsoft Teams.

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.
Pay per intercom per month or year, no additional Microsoft Teams licenses necessary!
Enjoy!

[Change plan](#)

Billing term 1-month subscription
 1-year subscription
 2-year subscription
 3-year subscription

Price + payment options

*Number of users (1-1000000)

Subtotal € 23,04743/user/1-month

Recurring billing On
 Off

[Review + subscribe](#) < Previous Next: Tags >

Useful links
[View this product in Marketplace](#)
[View all your SaaS subscriptions](#)

View this product in Marketplace
[View all your SaaS subscriptions](#)

Azure portal, CyberGate details

- Review all details, accept the terms of use and click 'Subscribe'.

Microsoft Azure

Home > CyberGate SIP intercom connect to Teams > **Subscribe To CyberGate SIP intercom connect to Teams**

Subscribe to plan

Basics Tags **Review + subscribe**

Product + plan details
CyberGate SIP intercom connect to Teams - CyberGate flex plan by CyberTwice B.V.
[Microsoft Standard Contract](#) | [Amendment](#) | [privacy policy](#)

Terms of use
By clicking "Subscribe" and completing the purchase with the provider, I (a) agree to the legal terms and privacy statement(s) associated with each Marketplace offering above, (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s), and (c) agree that Microsoft may share my contact information and transaction details (including usage volume associated with the offering) with the seller(s) of the offering(s).

Give Microsoft permission to use and share my contact information so that Microsoft or the Provider can contact me

Contact details

Name: Koos Ridder

Primary email address *: k...er@...s.com

Primary phone number *: 002...9

Basics

| | |
|-------------------------|---|
| Subscription | Microsoft Partner Network |
| Resource Group | Rc...eg |
| Name | CyberGate...s |
| Plan | CyberGate flex plan |
| Billing term | 1-month |
| Price + payment options | First month free, then €17.57/user/one-time payment |
| Number of users | 1 |
| Subtotal | €17.57/user |
| Recurring billing | On |

Subscribe < Previous: Tags Next >

Azure portal, CyberGate review

Microsoft Azure

Home > CyberGate SIP intercom connect to Teams > Subscribe To CyberGate SIP intercom connect to Teams > **Subscription progress**

Your SaaS subscription is in progress

SaaS resource name: CyberGate...s

Purchase start time: Wednesday, May 4, 2022, 2:48:14 PM

Offer & plan details: CyberGate SIP intercom connect to Teams - CyberGate flex plan - 1-month

Next steps (available once subscribed)

Configure SaaS account

To complete the purchase, configure your SaaS account on the publisher's website.

[Configure account now](#)

Important to know

Billing will start after your account is configured on the publisher's website.

If no action is taken within 30 days, this SaaS subscription will be automatically deleted.

Your SaaS subscription will appear on the [SaaS](#) page in the Azure portal. To access it easily, save it to your favorite services or pin it to the dashboard.

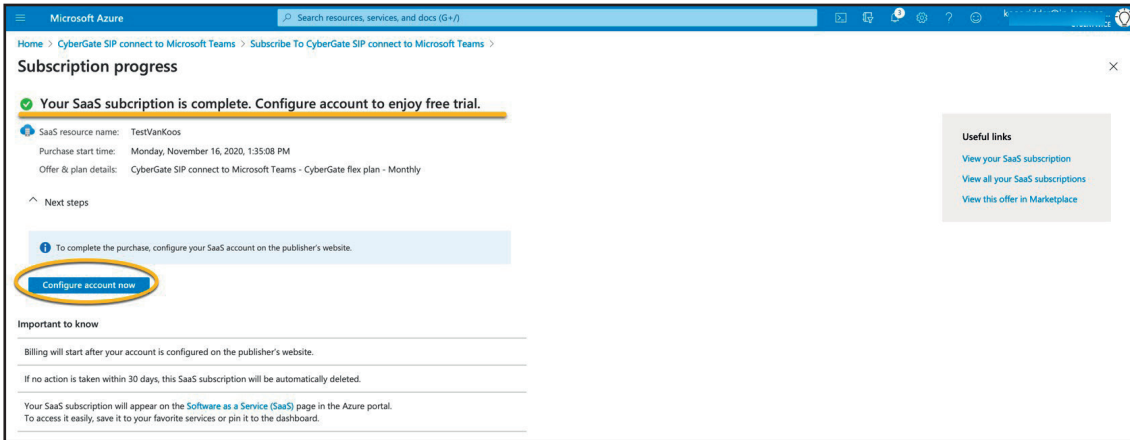
SaaS subscription is in progress
Your SaaS subscription 'CyberGateKooos' is in progress...

Useful links
[View your SaaS subscription](#)
[View all your SaaS subscriptions](#)
[View this product in Marketplace](#)

Azure portal, subscription is in progress

Wait for the subscription to finish.

- Click 'Configure account now' to finish the configuration of CyberGate



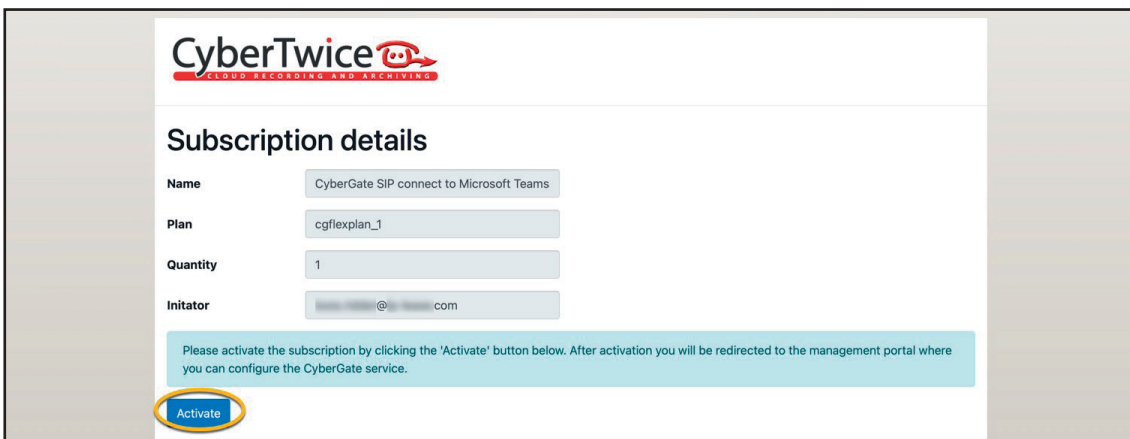
SaaS subscription complete

Azure Marketplace will redirect you to the CyberGate Management Portal where you can activate your CyberGate Purchase.

Note:

Log in with a user with **global administrator privileges** of your organization, this is mandatory to activate CyberGate. 

- View the subscription details and click 'Activate'. This will take you to the dashboard of the admin portal.



CyberGate overview of the 'Subscription details'

CyberTwice
CLOUD RECORDING AND ARCHIVING

Subscription details

Name: CyberGate SIP connect to Microsoft Teams

Plan: cgflexplan_1

Quantity: 1

Initiator: [redacted]@[redacted].com

Please activate the subscription by clicking the 'Activate' button below. After activation you will be redirected to the management portal where you can configure the CyberGate service.

Activate Subscription successfully activated!

CyberGate successfully activated

The CyberGate Management Portal will open and show the License overview.

CyberTwice Koos Ridder
fr[redacted]@in.onmicrosoft.com

License overview

| Name | Created | Quantity | Enabled |
|--|------------|----------|---------|
| fr[redacted]@in.onmicrosoft.com subscription | 2024-08-06 | 1 | yes |

CyberGate Management Portal License overview

Continue with Step 2: “Step 2: Configure CyberGate in the Management portal” on page 19.

Step 2: Configure CyberGate in the Management portal

The CyberGate Management Portal can be accessed here: <https://admin.cybergate.cybertwice.com>

The portal is divided into multiple sections, shown in the sidebar.

Note:

Follow the steps in this chapter for the basic configuration of CyberGate.

For a detailed description of the CyberGate Management portal, please see **Appendix A: How to use the CyberGate Management Portal** in this document.



Steps to follow

“Provide Admin Consent” on page 20

Provide Admin Consent to CyberGate. This has to be done by a Global Administrator

“Network settings” on page 21

Configure the Public WAN IP address that the device uses to connect to CyberGate

“Device settings” on page 22

Create a device in CyberGate. This will generate the details needed to configure the devices' SIP settings

Continue with the device configuration using the device specific CyberGate manual

Provide Admin Consent

Global settings

In the section 'Global' you have to grant CyberGate limited access to your Azure environment. This is mandatory to be able to call Teams users in your organisation.

- Use the 'Provide admin consent' button to grant the set of access rights

Note:

You have to be an Global administrator to provide admin consent!



The screenshot shows the CyberTwice management portal. The left sidebar has a 'Global' menu item circled in yellow. The main content area is titled 'Global settings' and has a sub-section 'Admin consent'. A yellow banner states: 'The CyberGate service needs to be granted a limited set of access rights to your Azure environment to function correctly. These rights have to be approved by a global administrator of your organization.' Below this, a blue button labeled 'Provide admin consent' is circled in yellow. Other sections visible include 'Communication Test Script' with a 'Download' button.

CyberGate management portal 'Global' - Provide admin consent

The screenshot shows the CyberTwice management portal after the admin consent step. The 'Global' menu item is still circled in yellow. The 'Admin consent' section is now circled in yellow and displays the message: 'Admin consent has been provided for this tenant.' The 'Communication Test Script' section remains visible with its 'Download' button. The 'Call forwarding' section is also visible, showing it is disabled with an 'Enable call forwarding' button.

CyberGate management portal 'Global' - Admin consent provided

- Click -Basic-Network- for the next step'.

Network settings

One of the security measures of CyberGate is a white list that contains the public WAN IP addresses used to connected to CyberGate. In order for a device to register with CyberGate, the public WAN IP-address your Device is using to connect to CyberGate has to be configured in the Basic-Network menu.

- Click 'Add WAN IP Address or Range'

The setting is saved automatically.

The screenshot shows the CyberTwice management portal interface. On the left is a navigation menu with categories: ADMINISTRATION (Licensing), BASIC (Global, Network, Portal access, SIP trunk, Device, Multi-ring), CAMERA (Meeting), and TEAMS APP (Availability, Device). The main content area is titled 'Network settings' and contains two sections: 'Configured WAN IP addresses' and 'Configured device location domain names'. Both sections have a yellow background and state 'No IP addresses configured.' and 'No domain names configured.' respectively. There are blue buttons for 'Add WAN IP Address or Range' and 'Add domain name'.

CyberGate management portal 'Network' - No WAN IP address configured yet

- Add the WAN IP address (optional: define a range of addresses)
- Add an optional description and / or location

This screenshot shows the same 'Network settings' page as above, but with a modal dialog box open. The dialog is titled 'Add WAN IP Address or Range' and contains the following fields: 'WAN IP Address Start' with a sub-label 'Enter IPv4 address' and a 'Use current WAN IP (62.233.198)' button; 'WAN IP Address End (optional)' with a sub-label 'Enter IPv4 address'; 'Description (optional)' with a sub-label 'Enter description' and a note 'The IP address description is used for administrative use only'; and 'Location (optional)' with a sub-label 'Enter location' and a note 'The IP address location is used for administrative use only'. At the bottom of the dialog are 'Cancel' and 'Add' buttons. In the background, the 'Network' menu item and the 'Add WAN IP Address or Range' button are circled in yellow.



CyberGate management portal 'Network' - Add WAN IP address or Range

CyberTwice Network settings

Configured WAN IP addresses

For security purposes the public WAN IP addresses used by devices to connect to the internet need to be set here. This is to allow a connection to the CyberGate service from the site where the device is installed. There is a maximum of 100 addresses that can be set here. Ranges count as multiple addresses.

[Add WAN IP Address or Range](#)

| IP Start ▲▼ | IP End | Description ▲▼ | Location ▲▼ | Enabled ▲▼ | Action |
|----------------|--------|---------------------|---------------|------------|---|
| 62.163.213.198 | | Demo WAN IP Address | Demo location | Yes |   |

CyberGate management portal 'Network' - WAN IP address configured

- Click 'Basic-Device' for the next step'.

Device settings

In the section 'Device' you will need to add a 'device' for each intercom/pager/camera you are using on this subscription. It will automatically generate a SIP username and SIP password that has to be used in your SIP device configuration.

- Click 'Add device'
- Configure:
 - Display Name (a descriptive name for this device)
 - Type (Intercom, Pager or Camera)
 - Location (location of the device)
- Click 'Add' to add this device

CyberTwice 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](#)

No devices configured. Please add a device which will be connected to the CyberGate service.

CyberGate management portal 'Device' - 'Add 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.

Feature configuration script

To make the display name visible and to enable calling from Teams to the device, 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](#)

Directly connected devices

[Add device](#)

| Display name | Authentication username | Password | Add-ons | Licensed | Recorded | Teams to device | Action |
|----------------------|-------------------------|--------------|---------|----------|----------|-----------------|---|
| <i>Varik</i> | | | | | | | |
| Development Intercom | LULML6 LXSC8SR1 | 2PL ●●●●●●●● | | yes | yes | yes | i e r |

CyberGate management portal 'Device' - 'Device added'

- Authentication username - The username is necessary when configuring the SIP device
- Password - The password is necessary when configuring the SIP device

Use the blue copy-buttons to conveniently copy the username and password in the device configuration when configuring your device. The Authentication username and the password are necessary to successfully register the device to CyberGate.

The Display name field will show the device name and will also show an explanation mark. The device *will* be able to call to Microsoft Teams, but will show the name 'Intercom' instead of the custom Display name until you execute the PowerShell script that can be downloaded on this page.

See **Appendix B Configure the display name of the device** for instructions on how to modify the display name from the default 'Intercom' to the Display name given.

Continue with Step 3: "Configure the device" on page 24.

Step 3: Configure the device

Now that CyberGate is ready, the next thing to do is configure the device. This step is done in the devices' own web interface. As each make / model device has its own configuration method, there are manuals for all certificated devices available.

[Click here for the download location](#) to all device installation manuals.

Manufacturers of compatible devices:

- **2N**
- **Akuvox**
- **Algo**
- **Alphatech**
- **Amphitech**
- **Axis**
- **Avigilon**
- **Barix**
- **BAS-IP**
- **Behnke**
- **Castel**
- **Commend**
- **Dnake**
- **Doorbird**
- **IPDoor**
- **Fanvil**
- **Fasttel**
- **Fermax**
- **Grandstream**
- **Hanwha**
- **Mobotix**
- **PortaDial**
- **Robin**
- **Suprema**
- **Valcom**
- **Verkada**
- **Zenitel**

When the instructions in the device installation manual are followed successfully, CyberGate is up and running and the device will be able to call Microsoft Teams users.

Appendix A: How to use the CyberGate Management Portal

The CyberGate Management Portal is the portal to configure CyberGate to fit your requirements. After CyberGate is activated you can login to the CyberGate Management portal at any time, as long as you log in with one of the following Microsoft admin accounts:

- Global-administrator
- Application administrator
- Cloud application administrator
- Teams administrator

Note:

You can also assign a Microsoft Group that contains one or more users that are also allowed to access the CyberGate Management Portal although they have no administrator rights. See 'Portal Access' for more information.



Use the CyberGate Management portal for:

- Licensing:
 - Increase / decrease the number of devices you would like to use to connect to Microsoft Teams. You don't have to go to Microsoft Marketplace or a Microsoft portal to change this, you can modify this amount easily in the CyberGate Management portal
- Global:
 - Set / modify global CyberGate settings
 - Enable / disable recording of calls globally
 - Download of the communication test script for diagnosing issues
- Network:
 - Manage allowed public WAN IP-adresses
- Portal access:
 - Manage access of non-admin users to the CyberGate Management Portal
- Device management:
 - Add / remove devices
 - Rename devices. This will change the identification of the device when calling to Microsoft Teams
 - Enable / disable the recording of calls per device
 - Enable / disable the option to call the device from Microsoft Teams
- Multi-ring:
 - Add / remove Multi-ring groups. A Multi-ring group allows you to ring multiple people in your organisation simultaneously
 - Modify Multi-ring groups
- CyberGate Teams app:
 - Modify settings related to the CyberGate for Teams app

The CyberGate Management portal consists of four main sections:

1. *Administration*
2. *Basic*
3. *Camera*
4. *Teams App*

Administration

The *Administration* section contains license related settings of the CyberGate subscription.

Licensing

Name

The name of the subscription

Created

The creation date of the subscription

Plan

The name of the chosen plan during CyberGate purchasing

Quantity

Shows the actual licensed amount of intercoms that can be used

Requested quantity

The amount of requested device licenses. Usually the 'Requested quantity' number is equal to the 'Quantity' number.

To increase or decrease the number of licensed devices, click on the blue 'edit' symbol and click on the '+' or '-' symbol. By increasing the number of licenced devices the monthly cost will also be increased, decreasing the number of licenced devices will decrease the monthly cost.

Enabled

If the CyberGate license is active and paid, the 'Enabled' status will show 'yes'. If it shows 'no', this subscription and the intercoms using this subscription will not work. In that case check the subscription in the Microsoft portal (<https://portal.microsoft.com>) for more details.

Note:

After modifying the amount of licenced devices, the 'Quantity' number might not be equal to the 'Requested quantity' number. It can take up to 10 minutes for Microsoft to implement the subscription change. After that, the numbers should be equal.



Basic

The *Basic* section allows you to modify general settings.

Global

CyberTwice Kees Ridder
C

ADMINISTRATION

- Licensing

BASIC

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

CAMERA

- Meeting

TEAMS APP

- Availability
- Device

Global settings

Admin consent
Admin consent has been provided for this tenant.

Communication Test Script
The Communication Test Script helps with troubleshooting possible connection problems between your local network and the online CyberGate service. This easy-to-run PowerShell script detects any connections that might be blocked by a firewall, NAT router or Sip gateway. This script can be downloaded with the button below.
[Download](#)

Call forwarding ⓘ
Call forwarding is disabled
The Teams call will not be forwarded to another user or user group, even if this is configured for the called Teams user. The voicemail will never answer the call. If this is not the desired behavior, the call forwarding can be enabled.
[Enable call forwarding](#)

Trunk Support ⓘ
SIP Trunk support is disabled
SIP Trunk support is necessary when your intercoms will be connected to the CyberGate service via a single SIP device. This is an advanced feature that most users don't need. Currently CyberGate only supports the 'Commod VirtuoSIS' SIP trunks. Please contact CyberTwice when you have questions regarding this feature.
[Enable trunk support](#)

Security policies ⓘ
Secure-only policy is disabled
The secure-only policy will enforce secure SIP communication using TLS 1.2 and encrypted audio/video for all the devices you connect to CyberGate. When enabled, connecting over UDP / TCP to CyberGate will not be possible anymore, only SIP TLS and SRTP will be allowed. Check if your intercom is certified to use SIP TLS and SRTP with CyberGate ([Compatibility list](#)) and configure your intercom using the manual listed.
When the policy is disabled, devices can communicate using both secure SIP TLS and unsecure UDP / TCP, as well as use encrypted and unencrypted audio/video.
[Enable secure-only policy](#)

Call recording ⓘ
Call recording is disabled.
Recordings are handled by the CyberTwice cloud service called Attest. If enabled, calls from all your devices are recorded. You can disable recording per device in the Device Settings menu.
Note that the feature configuration script must have been executed for the recording to work.
[Enable call recording](#)

Audit trail
[Show](#)

CyberGate management portal 'Global' - 'Admin consent' provided

Admin consent

Admin consent has to be provided for CyberGate to be able to communicate to the Teams environment of the tenant. This is already done during the CyberGate purchase and configuration. Future updates of CyberGate might require updating the Admin consent to activate new features.

Communication Test Script

The Communication Test Script helps with troubleshooting possible connection problems between your local network and the online CyberGate service. This easy-to-run PowerShell script detects any connections that might be blocked by a firewall.

Call forwarding

The 'Call Forwarding' option in this section enables / disables calls to Teams users that are forwarded to other users or to the Teams voice mail system.

By default, calls to forwarded destinations (such as voice mail) are ignored. Therefore a call from the device will not be answered by the voice mail system.

If a Teams user has its account forwarded to another Teams user, call forwarding should be enabled to make it work. Keep in mind that this will also enable call forwarding to the Teams voice mail system.

Trunk Support

The 'Trunk Support' option enables the possibility to connect SIP trunks to CyberGate. SIP Trunk support is necessary when your intercoms are connecting via another device that connects to CyberGate. This is usually called a SIP trunk. Please contact CyberTwice when you have questions regarding this feature.

Security Policies

The secure-only policy will enforce secure SIP communication using TLS 1.2 and encrypted audio/video for all the devices you connect to CyberGate. When enabled, connecting over UDP / TCP to CyberGate will not be possible anymore, only SIP TLS and SRTP will be allowed.

Note:

When the policy is disabled, devices can communicate using both secure SIP TLS and unsecure UDP / TCP, as well as use encrypted and unencrypted audio/video.



Call recording

Recordings are handled by the CyberTwice cloud service called Attest. When enabled, calls from all your devices will be recorded. You can disable recording per device in the Device section.

See **Appendix C: Call Recording** in this document for information about the recording feature and instructions on how to use it.

Note:

Please check the applicable national and state legislation and regulations related to Call Recording before activating this feature.



Audit Trail

The audit trail shows all user activity in the CyberGate Management portal.

Network

The *Network* section lets you configure your CyberGate white-list.


One of the security measures of CyberGate is a white list that contains the public WAN IP addresses used to connected to CyberGate.

In order for a device to register with CyberGate, the public WAN IP-address your intercom is using to connect to CyberGate has to be configured in the Basic-Network menu.

Note:

The network section also features an option to add 'Configured device location domain names'. This option is currently limited to users of the Genetec Sipelia Cloud deployments.



CyberTwice  Koos Ridder
InOntwikkeling ▼

ADMINISTRATION

- Licensing

BASIC

- Global
- Network**
- Portal access
- SIP trunk
- Device
- Multi-ring

CAMERA

- Meeting

TEAMS APP

- Availability
- Device

Network settings

Configured WAN IP addresses

For security purposes the public WAN IP addresses used by devices to connect to the internet need to be set here. This is to allow a connection to the CyberGate service from the site where the device is installed. There is a maximum of 100 addresses that can be set here. Ranges count as multiple addresses.

[Add WAN IP Address or Range](#)

No IP addresses configured.

Configured device location domain names


Domain names can be configured to be resolved as WAN IP addresses of device locations. Only use this when no static (fixed) WAN IP is available.

[Add domain name](#)

No domain names configured.

CyberGate management portal 'Network' - 'Nothing configured'

- To add one or more WAN IP addresses, click 'Add WAN IP Address or Range'

CyberTwice  Koos Ridder
InOntwikkeling ▼

ADMINISTRATION

- Licensing

BASIC

- Global
- Network**
- Portal access
- SIP trunk
- Device
- Multi-ring

CAMERA

- Meeting

TEAMS APP

- Availability
- Device

Network settings

Configured WAN IP addresses

For security purposes the public WAN IP addresses used by devices to connect to the internet need to be set here. This is to allow a connection to the CyberGate service from the site where the device is installed. There is a maximum of 100 addresses that can be set here. Ranges count as multiple addresses.

[Add WAN IP Address or Range](#)

No IP addresses configured.

Configured device location domain names

Domain names can be configured to be resolved as WAN IP addresses of device locations. Only use this when no static (fixed) WAN IP is available.

[Add domain name](#)

No domain names configured.

Add WAN IP Address or Range ✕

WAN IP Address Start

[Use current WAN IP \(62.233.198\)](#)

WAN IP Address End (optional)

Description (optional)

The IP address description is used for administrative use only

Location (optional)



The IP address location is used for administrative use only

[Cancel](#) [Add](#)

CyberGate management portal 'Portal access' - 'Add IP address'

- Add the WAN IP address (optional: define a range of addresses)
- Add an optional description and / or location

The screenshot shows the CyberTwice management portal interface. The left sidebar contains navigation menus for ADMINISTRATION, BASIC, CAMERA, and TEAMS APP. The main content area is titled 'Network settings' and includes a section for 'Configured WAN IP addresses'. Below this section is a table with the following data:

| IP Start ▲▼ | IP End | Description ▲▼ | Location ▲▼ | Enabled ▲▼ | Action |
|-------------|--------|----------------|-------------|------------|---|
| 62.16 | 33.198 | Building A | Amsterdam | Yes |   |

Below the table, there is a section for 'Configured device location domain names' with a message: 'No domain names configured.'

CyberGate management portal 'Portal access' - 'IP Address added'

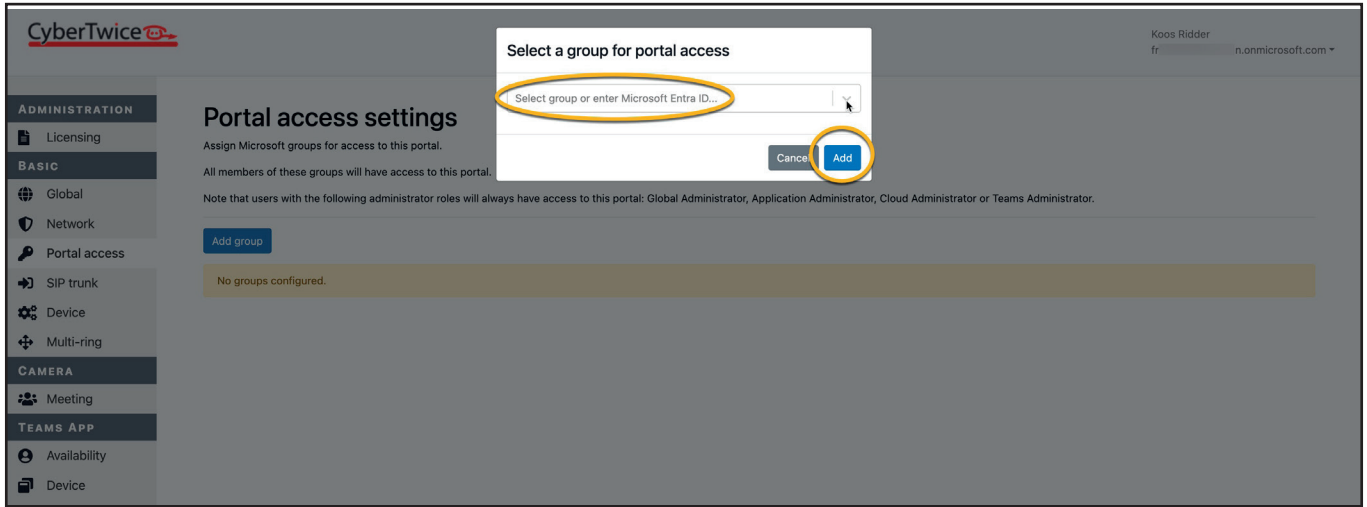
Portal access

The *Portal access* section lets you modify access to the CyberGate Management Portal. It allows non-admin users to log in to the CyberGate Management Portal.

The screenshot shows the CyberTwice management portal interface. The left sidebar contains navigation menus for ADMINISTRATION, BASIC, CAMERA, and TEAMS APP. The main content area is titled 'Portal access settings' and includes a section for 'Add group'. Below this section is a message: 'No groups configured.'

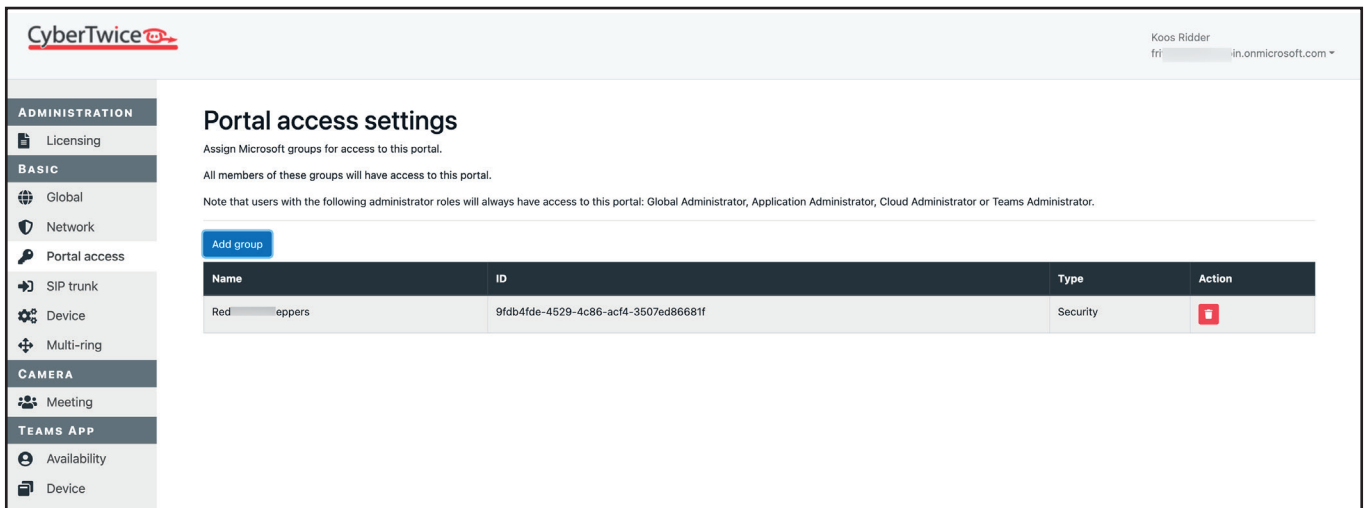
CyberGate management portal 'Portal access' - 'No group added yet'

- Click 'Add group' to grant a group access to the portal.



CyberGate management portal 'Portal access' - 'Select group'

- Pick a group from the drop down menu or enter the group-ID to add.



CyberGate management portal 'Portal access' - 'Group added'

Device

The *Device* section lets you add, modify or delete devices that connect to CyberGate.

Download

To download the feature configuration script, click on the blue 'Download' button. The feature configuration script is necessary to change the name of a device and enables other features such as the ability for call recording, the ability to call the device from Teams and use the Open door feature of CyberGate.

Add a device

To add a new device, click on the blue 'Add device' button. It will open a dialog box to configure the new device and will automatically generate a SIP username and SIP password that can be used in the device.

Add Device [X]

Username & password
The username and password for your device are automatically generated when a device is added.

Display name
Enter display name
This name is used as a display name within Teams

Type
Intercom
The device type is used for administrative use only

Location
Enter location
The device location is used for administrative use only

Record device

Recording is disabled globally. Enable recording in the tenant settings menu.

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)
Enter open-door code
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 # *).

Cancel Add

CyberGate management portal 'Device' - 'Add device'

Modify a device

Click on the blue edit-symbol to edit the device settings. After changing the device name, you'll have to download and execute the PowerShell script on this page using the download link.

Note:

Refer to the Appendix B: Configure the display name of the device for instructions on how to modify the display name from the default 'Intercom' to the Display name given.



Delete a device

To remove a device, click on the red trash can symbol to delete it. This action can not be undone.

Each device added shows:

- *A display name* - The display name is the name that will be shown in Microsoft Teams when the device calls a Teams user
- *Authentication username* - The username is necessary when configuring the device *
- *Password* - The password is necessary when configuring the device *
- *Add ons* - Shows the (optional) installed Add-ons for this device
- *Licensed* - You can create more devices than your subscription allows. In that case the devices that exceed the number of devices on your subscription will show 'Licensed - no' and will not work. As soon as you increase the amount of intercoms on your subscription the device licensed state will change to 'yes'
- *Recorded* - Indicates if recording for this device is enabled or not
- *Teams to device* - Indicates if the Teams to device feature (makes it possible to call the device from the Teams client) for this device is enabled or not

Note:

Use the blue copy-buttons to conveniently copy the username and password in the device configuration when configuring your device.



CyberTwice Kees Ridder
InOntwikkeling ▼

ADMINISTRATION

- Licensing

BASIC

- Global
- Network
- Portal access
- SIP trunk
- 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.

Feature configuration script

To make the display name visible and to enable calling from Teams to the device, 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

Directly connected devices

Add device

| Display name | Authentication username | Password | Add-ons | Licensed | Recorded | Teams to device | Action |
|----------------------|-------------------------|----------|---------|----------|----------|-----------------|--------|
| Vanik | | | | | | | |
| Development Intercom | LULML6 | LXSCBSR1 | 2PL | yes | yes | yes | |

CyberGate management portal 'Device' - 'Device added'

Note:

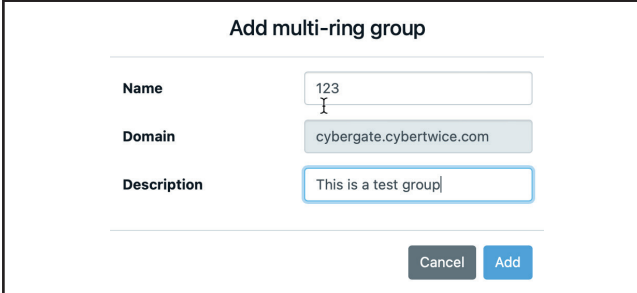
If the Display name field will show the name and show an explanation mark symbol, the device will be able to call to Microsoft Teams, but will show the name 'Intercom' instead of the custom Display name until you execute the PowerShell script that can be downloaded on this page.

See **Appendix B: Configure the display name of the device** for instructions on how to modify the display name from the default 'Intercom' to the Display name given.

Multi-ring

The multi-ring section lets you configure a group of Teams users to call as if it was one destination. This way multiple Teams users will be notified simultaneously if someone rings the intercom. The 1st responder will be connected to the visitor.

- Click 'Add multi-ring group' to create a multi-ring group.



The screenshot shows a form titled "Add multi-ring group". It contains three input fields: "Name" with the value "123", "Domain" with the value "cybergate.cybertwice.com", and "Description" with the value "This is a test group". At the bottom right, there are two buttons: "Cancel" and "Add".

CyberGate management portal 'Add multi-ring group'

- Name the Multi-ring group and add a description

The name combined with the fixed domain: cybergate.cybertwice.com will make the call destination. E.g.: If the name is 123, the name to dial in the intercom will be: 123@cybergate.cybertwice.com.

Note:

The domain part of the Multi-ring group is always cybergate.cybertwice.com, this is because the Multi-ring group is a CyberGate feature and not a Microsoft Teams domain feature.

Add the required Teams users to the Multi-ring group. The setting will be saved automatically. You can copy the group name by clicking the blue 'Copy to clipboard' icon.

The screenshot shows the 'Multi-ring settings' page in the CyberTwice management portal. The left sidebar contains navigation menus for 'ADMINISTRATION', 'BASIC', 'CAMERA', and 'TEAMS APP'. The main content area is titled 'Multi-ring settings' and includes a notice about the Microsoft Teams app. A blue button labeled 'Add multi-ring group' is visible. Below it, a form shows a group named '123@cybergate.cybertwice.com' with the description 'This is a test group'. A yellow message states 'This multi-ring group does not yet contain any participants.' At the bottom of the form, there is an input field, an '@' symbol, a dropdown menu showing 'fr' and 'in.onmicros', and an 'Add' button.

CyberGate management portal 'Multi-ring' - 'Multi-ring group added'

This screenshot shows the same 'Multi-ring settings' page, but now a user has been added to the group. The group name '123@cybergate.cybertwice.com' and description 'This is a test group' remain. Below the yellow message, a table lists the added user: 'Teams username' with the value 'koos@fr[redacted]n.onmicrosoft.com' and a 'Delete' button. The 'Add' button at the bottom of the form is still present.

CyberGate management portal 'Multi-ring' - 'User added to the Multi-ring group'

SIP trunk settings

The *SIP trunk settings* section is only visible when the option 'Enable trunk support' in the Global section is enabled.

SIP trunk settings lets you add and delete one or more SIP trunks or modify the name of a SIP trunk.

Note:

SIP trunks can only be used with Comend and Genetec. Other manufacturers currently don't offer CyberGate certified SIP trunks.



When using a SIP trunk to connect to CyberGate, CyberGate will detect all the devices that are calling through that SIP trunk and will automatically add these devices to the SIP trunk section of the Device section.

The screenshot shows the CyberTwice management portal interface. The left sidebar contains a navigation menu with categories: ADMINISTRATION (Licensing), BASIC (Global, Network, Portal access, SIP trunk, Device, Multi-ring), CAMERA (Meeting), and TEAMS APP (Availability). The 'SIP trunk' item is highlighted with a yellow circle. The main content area is titled 'SIP trunk settings' and includes a sub-header: 'The incoming credentials for your trunks are automatically generated when a trunk is added. Separate outgoing credentials can be provided in case the outgoing requests require different credentials than the incoming requests.' Below this is a table with the following data:

| Name | Incoming username | Incoming password | Outgoing username | Outgoing password | Auto discover | Devices | Action |
|------------|-------------------|-------------------|-------------------|---------------------------|---------------------------|---------|--------|
| Test trunk | 99RW4IP | YMHGDF | 3H2 | Incoming username is used | Incoming password is used | Enabled | 0 |

CyberGate management portal 'SIP trunk' - One SIP trunk configured

Each created SIP trunk generates its own Authentication username and Password. This information can be easily copied using the blue 'copy to clipboard' buttons and can be used in the SIP configuration of the SIP trunk.

Outgoing username and Outgoing password

Some SIP trunks -such as Genetec Sipelia- require credentials to communicate back to the SIP trunk. Modify these credentials by clicking the blue edit-symbol.

Modify a SIP trunk

Click on the blue edit-symbol to edit the name of the SIP trunk.

Delete a SIP trunk

To remove a SIP trunk, click on the red trash can symbol to delete it. This action can not be undone.

Note:

A SIP trunk can not be deleted if there are devices that use this SIP trunk. In that case delete these devices in the Device section before deleting the SIP trunk.



Camera

The *Camera* section allows you to modify settings regarding to cameras.

Meeting

The meeting feature allows a device to join an existing meeting. If the device is configured to use the Meeting feature, it will automatically join a meeting instead of calling a Teams user. This meeting can then be joined by one or more Teams users to allow them all to access the audio and video of the device.

It is also possible to configure the Meeting feature so that Teams users are automatically called in to the meeting when a device joins the meeting.

The screenshot shows the CyberTwice management portal. The left sidebar contains a navigation menu with categories: ADMINISTRATION (Licensing), BASIC (Global, Network, Portal access, SIP trunk, Device, Multi-ring), CAMERA (Meeting), and TEAMS APP (Availability, Device). The 'Meeting' option under the CAMERA category is circled in yellow. The main content area is titled 'Meeting settings' and includes a blue 'Add meeting' button.

CyberGate management portal 'Meeting' - 'No meeting configured yet'

- Click 'Add meeting' to create a meeting.

Add meeting

| | |
|--------------------------|---|
| Name | <input type="text"/> |
| Domain | <input type="text" value="cybergate.cybertwice.com"/> |
| Description | <input type="text"/> |
| Teams meeting URL | <input type="text"/> |

CyberGate management portal 'Meeting' - 'Add meeting'

- Name the Meeting, add a description and a Teams meeting URL
- The Teams meeting URL field accepts the URL of a Teams meeting *
- All Teams users that are invited in- or part of this meeting will receive a notification when the device joins the meeting.

* You can create a new meeting in Teams, and copy its URL in this field. You can also use the URL of an existing Teams meeting.

To automatically call Teams users (instead of only notifying them) you can add them to this meeting:

- Enter their Teams name, selecting the domain and clicking the blue 'Add' button.

The screenshot displays the 'Meeting settings' interface in the CyberTwice management portal. On the left, a sidebar contains navigation menus for 'ADMINISTRATION', 'BASIC', 'CAMERA', and 'TEAMS APP'. The main area shows a 'Meeting settings' section with an 'Add meeting' button. Below this, a meeting configuration box is visible, showing the meeting name 'Meeting test' and its URL. A table lists added users, with one user 'ridderkoos@In...g.onmicrosoft.com' already added. At the bottom, there is a form to add a new user, with the 'Add' button highlighted by a yellow circle.

CyberGate management portal 'Meeting' - One user added. (will be called automatically when the device joins the meeting)

Teams App

The *Teams App* section allows you to set permissions for the *CyberGate for Teams app*.

Note:

The CyberGate for Teams app is an app developed to run from within Microsoft Teams. It can be downloaded from within the Teams client via the App-menu.

Direct link to the CyberGate for Teams app: [Link](#)

The CyberGate for Teams app allows Teams users to set their Multi-ring group availability and to view all devices connected to CyberGate and quickly initiate calls to these devices

The settings in this menu are designed to set permissions for this functionality. You can:

- Limit who can see devices in the CyberGate for Teams app
- Assign a 'Supervisor' that is in charge of a Multi-ring group.

A Supervisor of a Multi-ring group can perform the following tasks in the CyberGate for Microsoft Teams app:

- Can add and delete users in this Multi-ring group
- Set the availability for all users in the Multi-ring group

Availability

The *Availability* section shows all created Multi-ring groups. By default a Multi-ring group does not have a Supervisor defined as this is an optional feature and not necessary for the functioning of a Multi-ring group.

Add a supervisor:

- Click on the blue edit-symbol to add one or more supervisors.

CyberTwice Kris Ric...
Kris Te...nt

ADMINISTRATION

- Licensing

BASIC

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

CAMERA

- Meeting

TEAMS APP

- Availability
- Device

Availability supervisor settings

Assign supervisors to a configured multi-ring group.

A supervisor can set the availability of every member of the multi-ring group in the 'Availability' tab of the CyberGate for Microsoft Teams app.

New Microsoft Teams app

- Set your personal availability for each configured multi-ring group.
- Find all your configured devices.

[Get CyberGate for Microsoft Teams App here](#)

| Multi-ring group | SIP address | Supervisor(s) |
|----------------------|------------------------------|---------------|
| This is a test group | 123@cybergate.cybertwice.com | |

CyberGate management portal 'Availability' - No Supervisor configured yet

Define supervisors of multi-ring group '123@cybergate.cybertwice.com'

Current supervisors

| Teams username | Delete |
|---------------------------------|--------|
| ric...s@InC...g.onmicrosoft.com | |

@ InC...g.onmicrosoft.com

CyberGate management portal 'Availability' - Select Supervisor

- Click 'Update' to save.

The screenshot shows the 'Availability supervisor settings' page in the CyberTwice management portal. The page title is 'Availability supervisor settings'. Below the title, there is a sub-header 'Microsoft Teams app' and a list of instructions: '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. Below this, there is a table with columns 'Multi-ring group', 'SIP address', and 'Supervisor(s)'. The table contains one row with the following data:

| Multi-ring group | SIP address | Supervisor(s) |
|----------------------|------------------------------|--------------------------------|
| This is a test group | 123@cybergate.cybertwice.com | • rirk@ms@ling.onmicrosoft.com |

CyberGate management portal 'Availability' - Supervisor configured

Device

The Device section shows all created devices. By default everyone can see a device in the CyberGate for Teams app. Restrict this access to a limited group of users by configuring one or more groups to a device. After adding a group to a device, it will only be visible for the users within the added group(s).

Add a group:

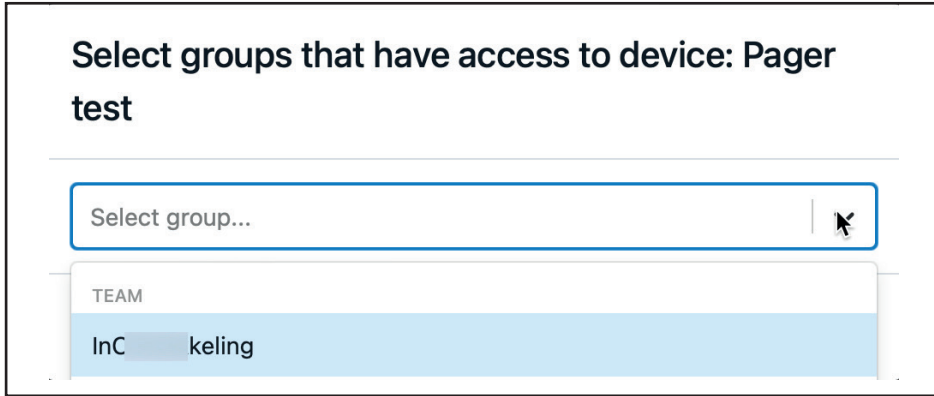
- Click on the blue edit-symbol to add one or more groups.

The screenshot shows the 'Device access settings' page in the CyberTwice management portal. The page title is 'Device access settings'. Below the title, there is a sub-header 'Microsoft Teams app' and a list of instructions: '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. Below this, there is a table with columns 'Device display name' and 'Microsoft group(s)'. The table contains one row with the following data:

| Device display name | Microsoft group(s) |
|---------------------|--------------------|
| Heerhugowaard | |
| Pager test | |

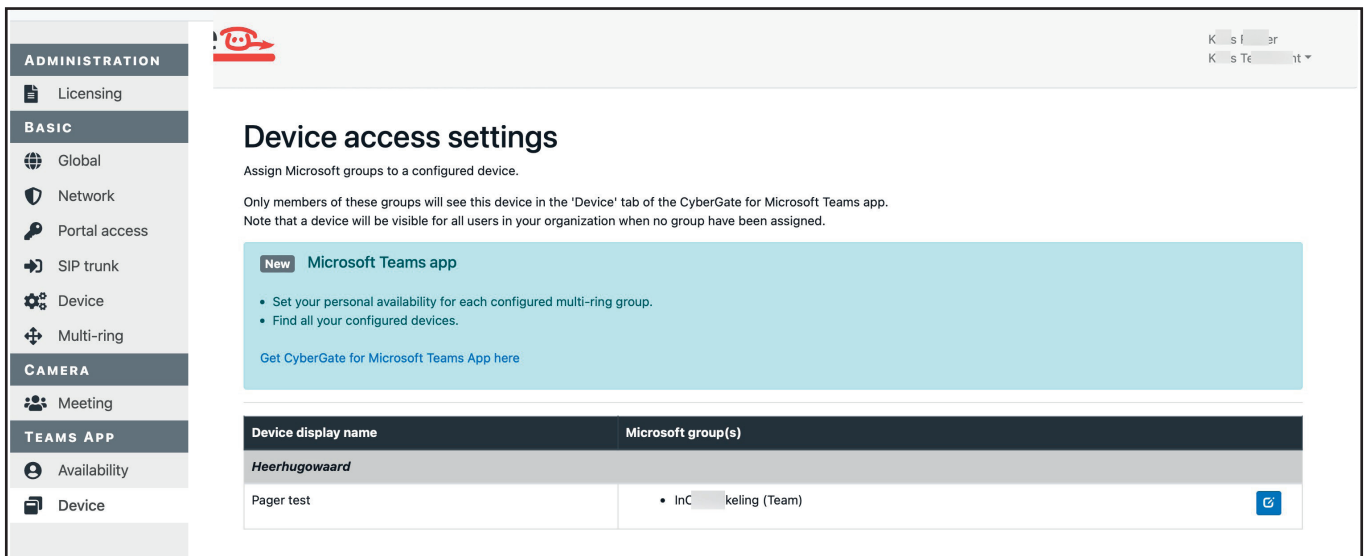
CyberGate management portal 'Device' - No Group configured yet

- Select a group or type to filter a group to add . All groups will be shown, Microsoft365, Security, Team, AAD groups.



CyberGate management portal 'Device' - Select Group

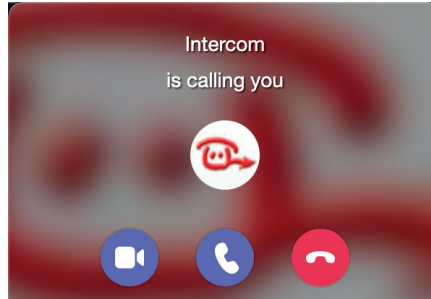
- Click 'Update' to save.



CyberGate management portal 'Device' - Group configured

Appendix B: Configure the display name of the device

By default, incoming calls from the device will be announced in Teams as 'Intercom'.



Microsoft Teams incoming call with the default name 'Intercom'

If you have multiple devices configured in CyberGate or you would like to show another name in Teams you can modify the name per configured device.

To do this, use the CyberGate Management Portal and navigate to the Basic-Device section.

CyberTwice

Koos Ridder
InOntwikkeling ▼

ADMINISTRATION

Licensing

BASIC

Global

Network

Portal access

SIP trunk

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.

Feature configuration script

To make the display name visible and to enable calling from Teams to the device, 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](#)

Directly connected devices

[Add device](#)

| Display name | Authentication username | Password | Add-ons | Licensed ! | Recorded | Teams to device | Action |
|----------------------|-------------------------|--------------|---------|---|----------|-----------------|--------|
| <i>Varik</i> | | | | | | | |
| Development Intercom | LULML6 LXSCBSR1 | 2PL ●●●●●●●● | | yes | yes | yes | |

CyberGate management portal 'Device' - Default 'Display name'

The Display name is the name that was configured during the adding of a the device to CyberGate. It can be modified using the blue edit button under 'Action'.

Update Device

Display name

This name is used as a display name within Teams

Type

Intercom

The device type is used for administrative use only

Location

The device location is used for administrative use only

Record device

Recording is disabled globally. Enable recording in the tenant settings menu.

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

Cancel Update

CyberGate management portal 'Device settings' - 'Update device'

CyberTwice Koos Ridder
InOntwikkeling ▼

ADMINISTRATION

- Licensing

BASIC

- Global
- Network
- Portal access
- SIP trunk
- 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.

Feature configuration script

To make the display name visible and to enable calling from Teams to the device, 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](#)

Directly connected devices

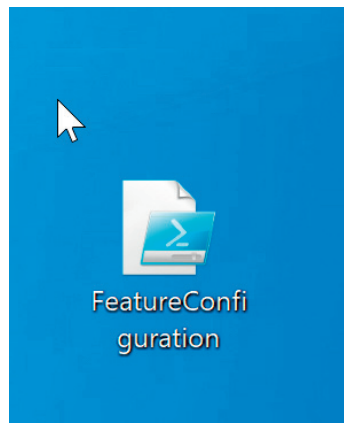
[Add device](#)

| Display name | Authentication username | Password | Add-ons | Licensed | Recorded | Teams to device | Action |
|----------------------|-------------------------|----------|---------|----------|----------|-----------------|--------|
| <i>Varik</i> | | | | | | | |
| Development Intercom | LULML6 | LXSC6SR1 | 2PL | yes | yes | yes | |

CyberGate management portal 'Device' - Custom 'Display name'

If the display name of the device shows the warning symbol, it is necessary to download and run the Feature configuration PowerShell script. If no warning sign is shown, skip this step.

1. Make sure you have a PC with Microsoft PowerShell installed.
2. Click on the blue 'Download' button to download the script

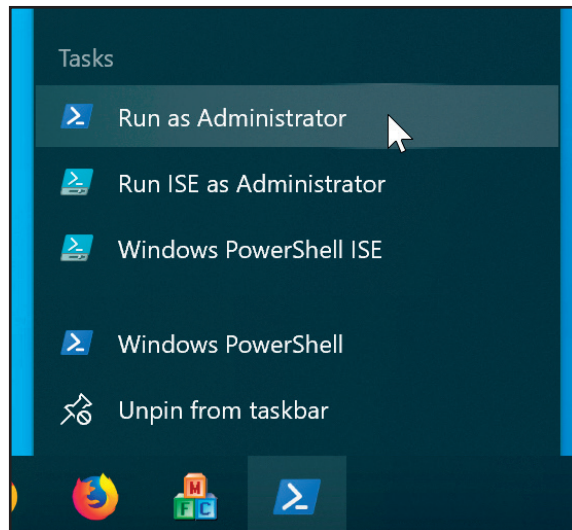


Microsoft Windows - Downloaded PowerShell script

3. Right-click on Powershell and select 'Run as Administrator.'

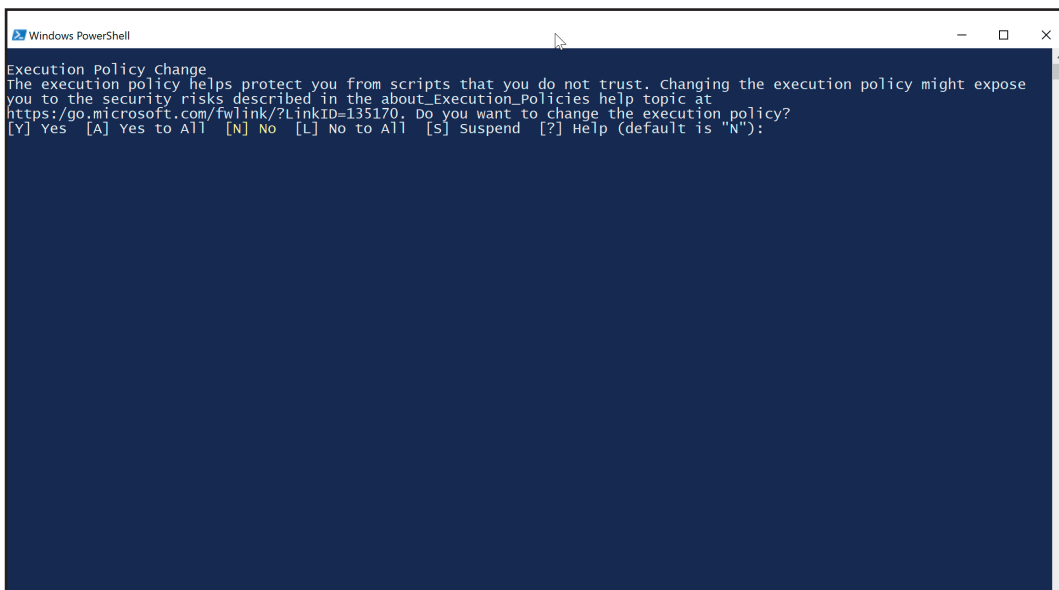
Note:

The downloaded script is customized and contains device information such as its display name. Do not re-use an earlier downloaded version of this script as this will result in a failure to modify the name of the device!



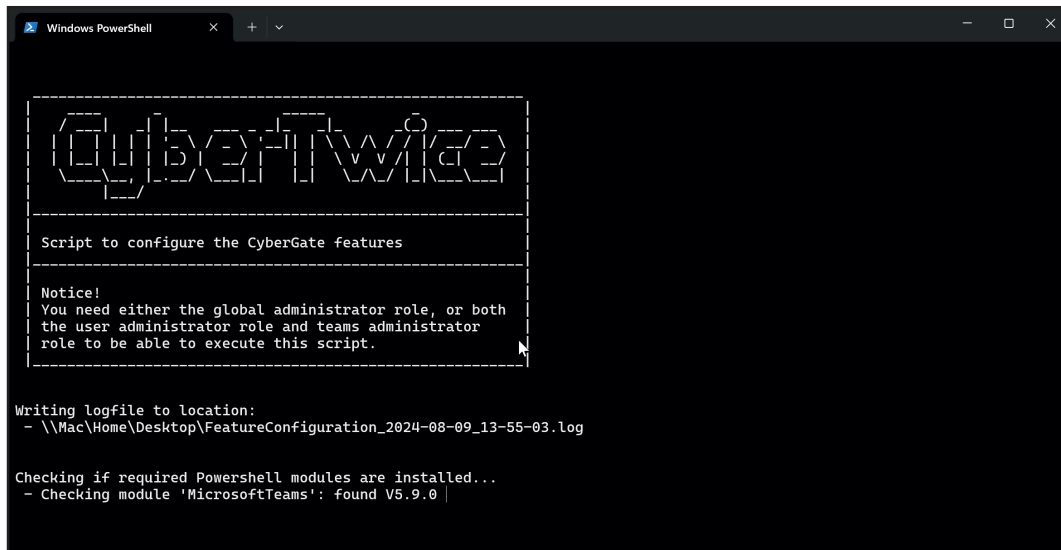
Microsoft Windows - 'Run as Administrator'

4. Depending on the Windows environment used a warning can be displayed. Select 'Yes' to execute this script.



Microsoft PowerShell - 'Execution Policy Change'

5. The script will ask you for your Microsoft account, this is by default the same account as used to configure CyberGate.



```
Windows PowerShell

CyberTwice

-----
Script to configure the CyberGate features
-----

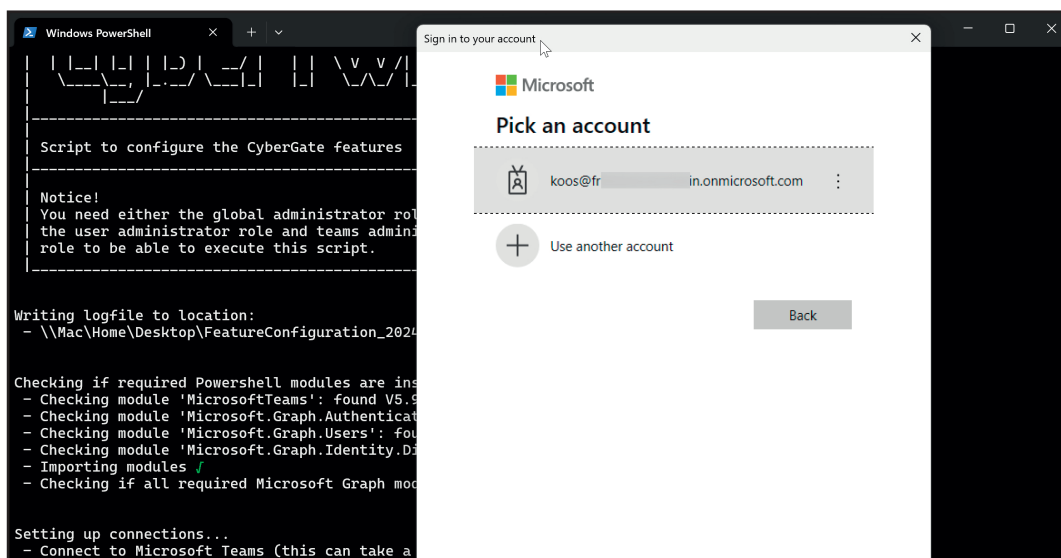
Notice!
You need either the global administrator role, or both
the user administrator role and teams administrator
role to be able to execute this script.

Writing logfile to location:
- \\Mac\Home\Desktop\FeatureConfiguration_2024-08-09_13-55-03.log

Checking if required Powershell modules are installed...
- Checking module 'MicrosoftTeams': found V5.9.0
```

Microsoft PowerShell - 'Azure user name'

6. Enter your password to login at Microsoft.



```
Windows PowerShell

Script to configure the CyberGate features

Notice!
You need either the global administrator role, or both
the user administrator role and teams administrator
role to be able to execute this script.

Writing logfile to location:
- \\Mac\Home\Desktop\FeatureConfiguration_2024-08-09_13-55-03.log

Checking if required Powershell modules are installed...
- Checking module 'MicrosoftTeams': found V5.9.0
- Checking module 'Microsoft.Graph.Authentication': found V1.5.0
- Checking module 'Microsoft.Graph.Users': found V1.5.0
- Checking module 'Microsoft.Graph.Identity.Directory': found V1.5.0
- Importing modules ✓
- Checking if all required Microsoft Graph modules are installed...

Setting up connections...
- Connect to Microsoft Teams (this can take a few minutes)
```

Sign in to your account

Microsoft

Pick an account

koos@fr in.onmicrosoft.com

Use another account

Back

Microsoft PowerShell - 'Login'

7. If you have two-factor authentication enabled, follow the steps asked for.
8. After successful authentication, the script will run and will display 'Script successfully done' if no errors occurred. Press Enter to exit the script.

```

01234567-1234-466f-9236-ce4a3d8d61dc aa/a493d-052b-4d4f-8775-1dde8f21592b
015b3c36-1ae9-466f-9236-ce4a3d8d61dc c84f2592-ebfa-47e7-b627-215d65d828bd
bdaa2e13-8f3d-4abd-aeel-a0757b7b1c38 92e7b15c-54c8-447f-af71-e715d1fab854
Note: It can take up to 1 hour before the configured display name(s) are visible in the Teams client.
Press Enter to continue...: |

```

Microsoft PowerShell - 'Script successfully done'

It can take up to an hour before the change will be in effect, up to that moment the device will be shown in Teams as 'Intercom'.
When in effect, the configured Display name will be displayed in Teams when the intercom operated.



Microsoft Teams incoming call with the new custom name

Appendix C: Call recording

CyberGate offers the option to record all intercom calls made through CyberGate. The recording feature is powered by the CyberTwice cloud service called *ATTEST*.

With call recording enabled, all calls made by your devices in CyberGate will be recorded by default, but can be disabled per device.

The recordings are securely stored in Microsoft Azure (West-Europe) for a period of 10 days, recordings older than 10 days will be deleted automatically.

The recordings are stored fully encrypted in the CyberTwice ATTEST Cloud service (Azure). To access the recordings ATTEST Replay is used.

ATTEST Replay offers an easy, convenient way of searching the recordings and playing them back.

You can access *ATTEST Replay* in three ways:

1. Via a link on the CyberGate Management portal
2. Via the Teams App store (within the Teams App), search for ATTEST Replay
3. Directly via this [Link to ATTEST Replay in Teams](#)

Note:

Please check the applicable national and state legislation and regulations related to Call Recording before activating this feature.



Steps to follow to enable recording in CyberGate

To enable recording follow the next steps:

“Activation of the recording feature” on page 52

Describes the procedure to enable the recording feature in the CyberGate Management Portal

“Search and replay recorded calls” on page 55

Describes ATTEST Replay to search and replay the recordings

“Modify the recording related settings” on page 59

Describes the recording related settings in the ATTEST Management Portal

Activation of the recording feature

The call recording feature can be enabled in the CyberGate Management Portal ([Link](#)).

- The first step is to login to the Cybergate Management portal using your Microsoft credentials and navigate to Basic-Global. Scroll down to the 'Call recording' section.

The screenshot shows the CyberTwice management portal interface. The left sidebar contains navigation menus for ADMINISTRATION, BASIC, CAMERA, and TEAMS APP. The 'Global' option under the BASIC menu is highlighted with a yellow circle. The main content area is titled 'Global settings' and includes sections for Admin consent, Configured WAN IP addresses, Communication Test Script, Call forwarding, Trunk Support, Security policies, and Call recording. The 'Call recording' section is at the bottom, with the 'Enable call recording' button highlighted by a yellow circle.

CyberTwice

ADMINISTRATION
Licensing

BASIC
Global
Network
SIP trunk
Device
Multi-ring

CAMERA
Meeting

TEAMS APP
Availability
Device

Global settings

Admin consent
Admin consent has been provided for this tenant.

Configured WAN IP addresses

| Address | Delete |
|----------------|--------|
| 62.1...2...198 | |

Other WAN IP address

Add additional WAN IP addresses.

Communication Test Script

The Communication Test Script helps with troubleshooting possible connection problems between your local network and the online CyberGate service. This easy-to-run PowerShell script detects any connections that might be blocked by a firewall, NAT router or Sip gateway. This script can be downloaded with the button below.

Call forwarding

Call forwarding is disabled

The Teams call will not be forwarded to another user or user group, even if this is configured for the called Teams user. The voicemail will never answer the call. If this is not the desired behavior, the call forwarding can be enabled.

Trunk Support

SIP Trunk support is enabled

SIP Trunk support is necessary when your intercoms are connecting via another device that connects to CyberGate. This is usually called a SIP trunk. Please contact CyberTwice when you have questions regarding this feature.

Security policies

Secure-only policy is disabled

The secure-only policy will enforce secure SIP communication using TLS 1.2 and encrypted audio/video for all the devices you connect to CyberGate. When enabled, connecting over UDP / TCP to CyberGate will not be possible anymore, only SIP TLS and SRTP will be allowed. Check if your intercom is certified to use SIP TLS and SRTP with CyberGate ([Knowledge base article](#)) and configure your intercom using the manual listed.

When the policy is disabled, devices can communicate using both secure SIP TLS and unsecure UDP / TCP, as well as use encrypted and unencrypted audio/video.

Call recording

Call recording is disabled.

Recordings are handled by the CyberTwice cloud service called Attest. If enabled, calls from all your devices are recorded. You can disable recording per device in the Device Settings menu.

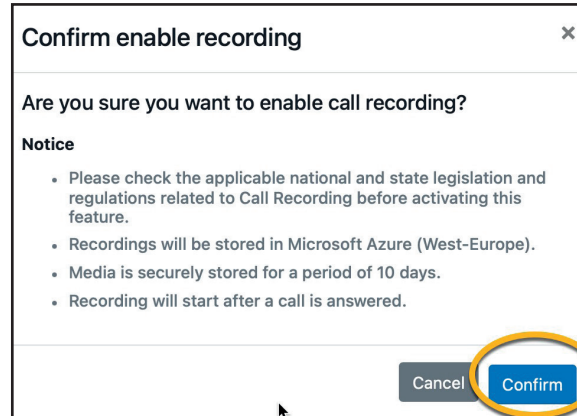
Note that the feature configuration script must have been executed for the recording to work.

CyberGate management portal 'Global' - Call recording disabled

- Click 'Enable call recording' to start the recording procedure

Note:

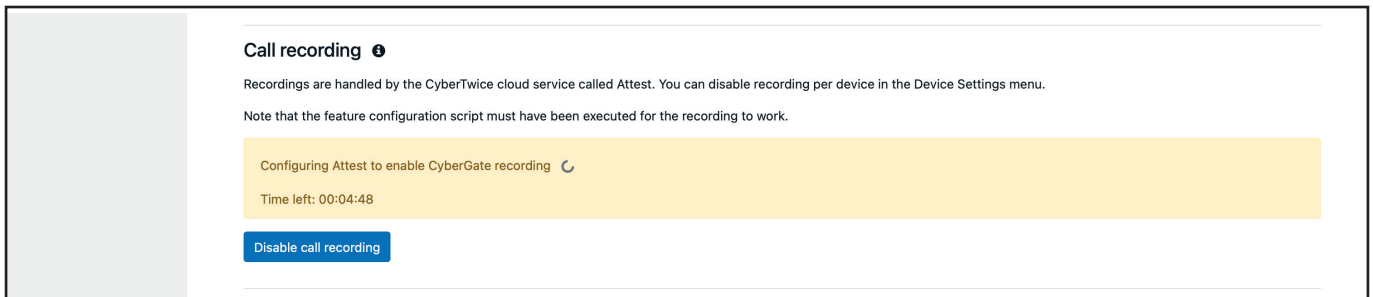
Call recording can only be enabled if the Feature Configuration PowerShell script has been run at least once. See Appendix B: Configure the display name of the device for instructions on how to run this script.



CyberGate management portal 'Global' - Confirm enable recording

- Click confirm to enable recording.

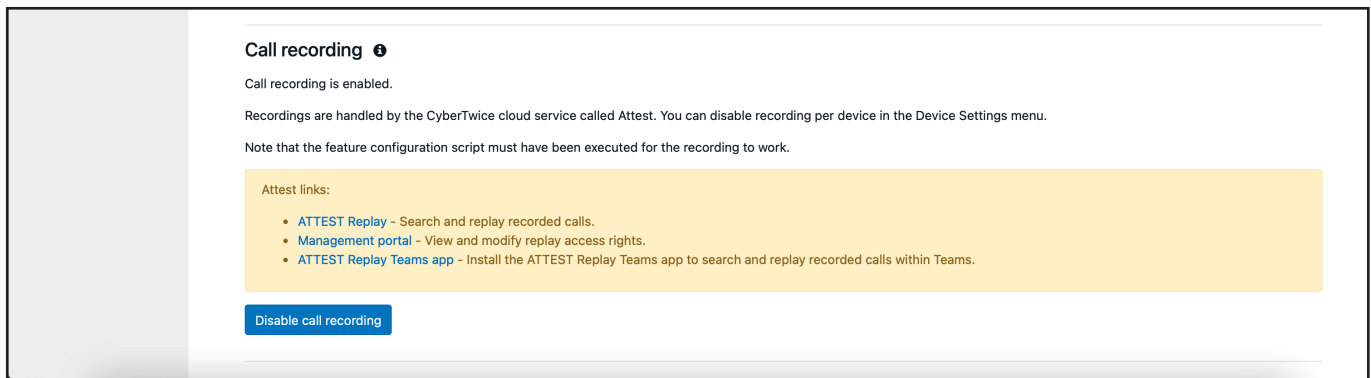
Recording will be set up for your Tenant. This can take up to 5 minutes.



CyberGate management portal 'Global' - Call recording configuring

After the recording is set up for your Tenant, three links will appear:

1. *Replay* - The website link to *ATTEST Replay*, the Search and Replay website where you can search calls, play them and see call transcriptions and -details. *Attest Replay* URL: [Link](#)
2. *Management portal* - The link to the management portal of *ATTEST*, where you can view and modify the access rights for call playback and change the selected transcription language. Management portal URL: [Link](#)
3. *ATTEST Replay Teams app* - Direct link to *ATTEST Replay* that runs directly in Microsoft Teams. Click this [Link](#) to install the app in your Microsoft Teams.



CyberGate management portal 'Global' - 'Recording enabled' window

The recording configuration is now complete! You can logout of the Cybergate Management portal and start using CyberGate with recordings.

Note:

It can take up to 15 minutes before a recorded call appears in ATTEST Replay.



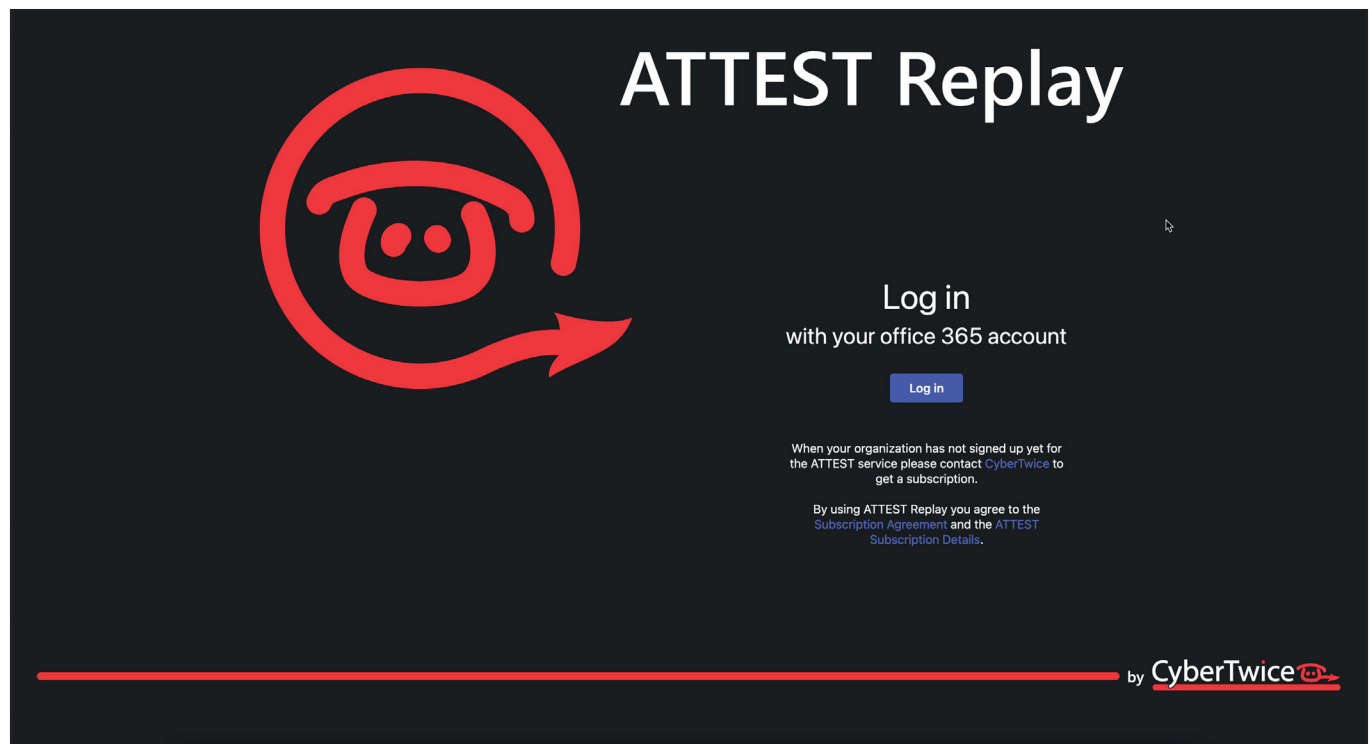
Search and replay recorded calls

The search and Replay of calls is done in the web application *ATTEST Replay*: [Link](#) or in the *ATTEST Replay Teams* app in Microsoft Teams: [Link to install ATTEST Replay in Teams](#)

Features:

- Find recordings fast using the Facet Search that lets you filter the recordings quickly
- Play the recordings

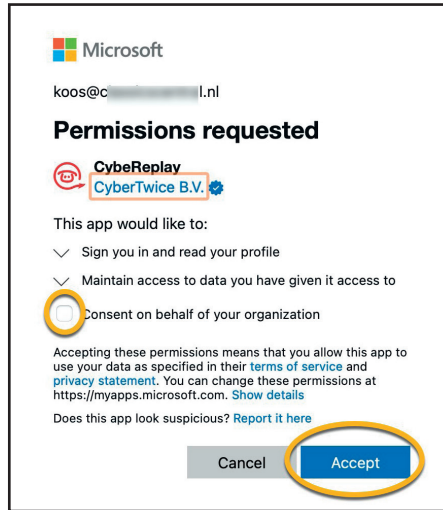
You can access ATTEST Replay using your Microsoft credentials.



ATTEST Replay login page

- Log in using your Microsoft credentials

- After logging in, a Microsoft Permission Request appears. Consent this either for your own account or for everyone in your organisation

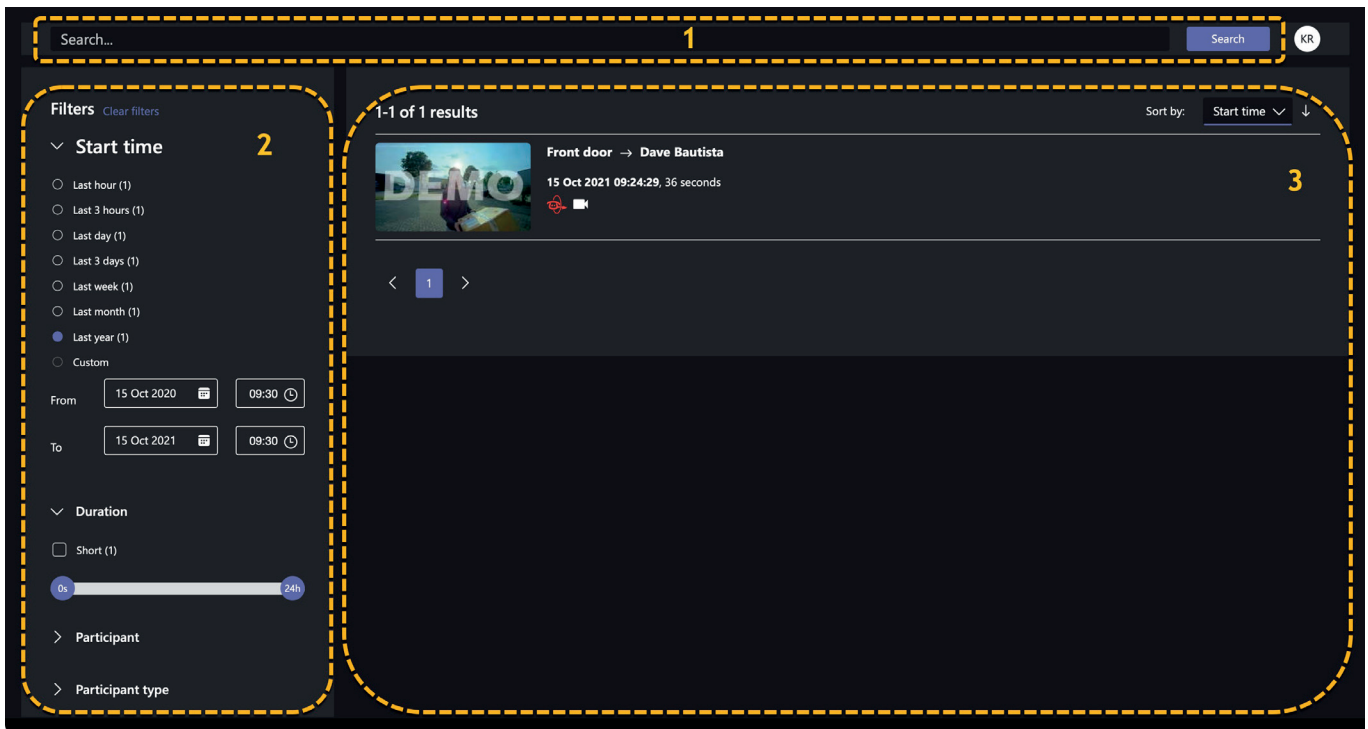


Microsofts 'Permissions requested' window - for ATTEST Replay

ATTEST Replay features a search screen and a replay screen. ATTEST Replay will open by default in the search screen.

The Search screen is divided into three main parts:

1. Search
2. Filters
3. Results



ATTEST Replay Search screen

1. Search

Search features a search bar and a search button that you can use to find recordings.

Use Search for:

- Names of participants in recording
- Words in the recordings transcribed text

2. Filters

Filters is a powerful tool to quickly filter search results. Select one or more items in Filters to display the results.

Note:

- *By selecting or deselecting an item in a filter, the search results and the other filters will be updated automatically*
- *The number displayed behind each filter indicate the number of results for that filter.*



3. Results

Results display all found recordings in a sortable card-style.

A card consists of:

- A preview
- The participants in the call
- The time and date of the recording
- The duration of the recording
- The recording type(s)

You can sort the calls by:

- Score, higher score = more relevant result
- Start time
- Duration
- User
- Number of participants

- Click on the card of the recording to play to open the replay window.



ATTEST Replay - Replay screen

The Replay screen opens. Here you can:

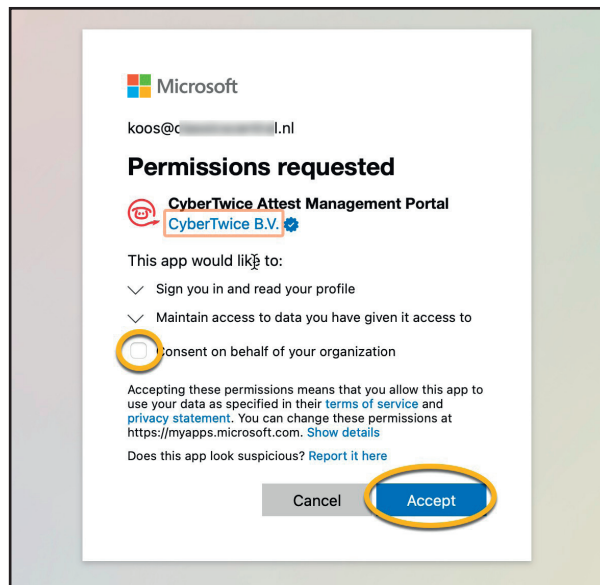
- See the Recording info
- See the Transcription of the recording with the option to follow the player (when available)
- Play the recording
- Pause the recording
- Skip through the recording
- Control the playback volume
- Enable / disable subtitles
- Change to full screen
- Return to the search results

Modify the recording related settings

The recording related settings can be modified in the management portal of ATTEST. The management portal of ATTEST can be accessed through this [link](https://admin.attest.cybertwice.com). (URL: <https://admin.attest.cybertwice.com>)

- Log into the ATTEST Management portal as an *Administrator*.

When logging in you'll be asked to accept the requested permissions. These are necessary for the portal to read your profile and display the data of the CyberGate recordings. You can choose to accept it only for you or for all administrators of your Tenant.



ATTEST management portal 'Permissions request'

When logged in successfully you'll be taken to the Subscription menu.

The screenshot shows the CyberTwice interface with the 'Subscription' menu selected. A table titled 'CyberGate' displays the following data:

| Name | Created | Plan | Auto renew | State |
|-----------|------------|-----------|------------|--------|
| CyberGate | 2024-01-03 | CyberGate | Yes | Active |

ATTEST management portal 'Subscription'

- Click on 'Dashboard' to show a graphical overview related to the recorded calls.

The screenshot shows the CyberTwice 'Dashboard' - 'Overview' tab. It features several data visualizations:

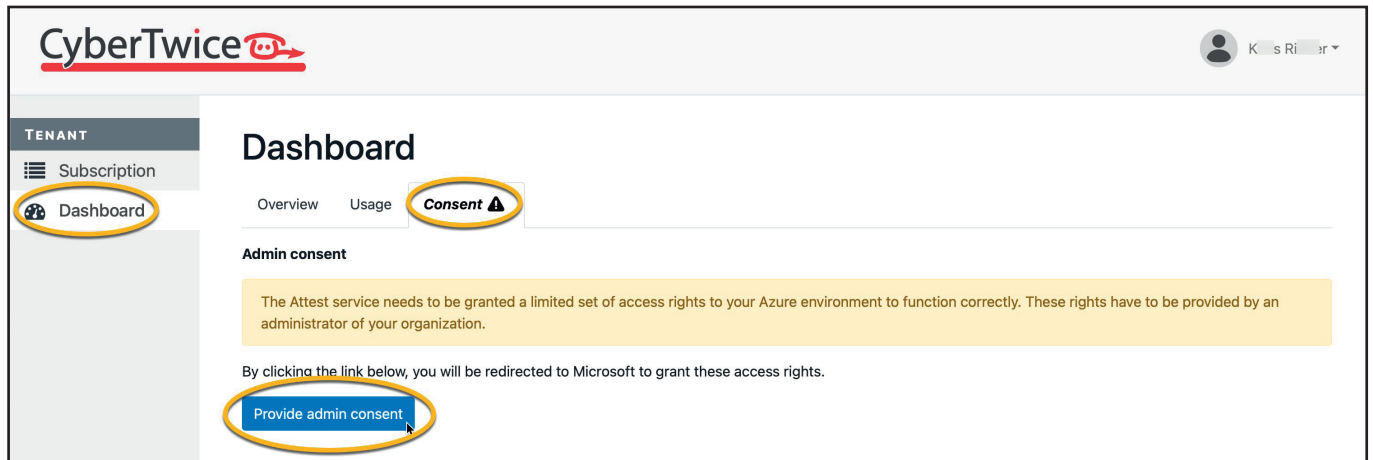
- Calls per user:** A pie chart showing a single slice for 'Front door'.
- Call volume:** A bar chart showing a total count of 1 call on Wednesday.
- Direction:** A partially visible pie chart.
- Call volume per type:** A bar chart showing a total count of 1 call.

The interface also includes a 'Last week' filter and navigation tabs for 'Overview', 'Usage', and 'Consent'.

ATTEST management portal 'Dashboard' - 'Overview' tab

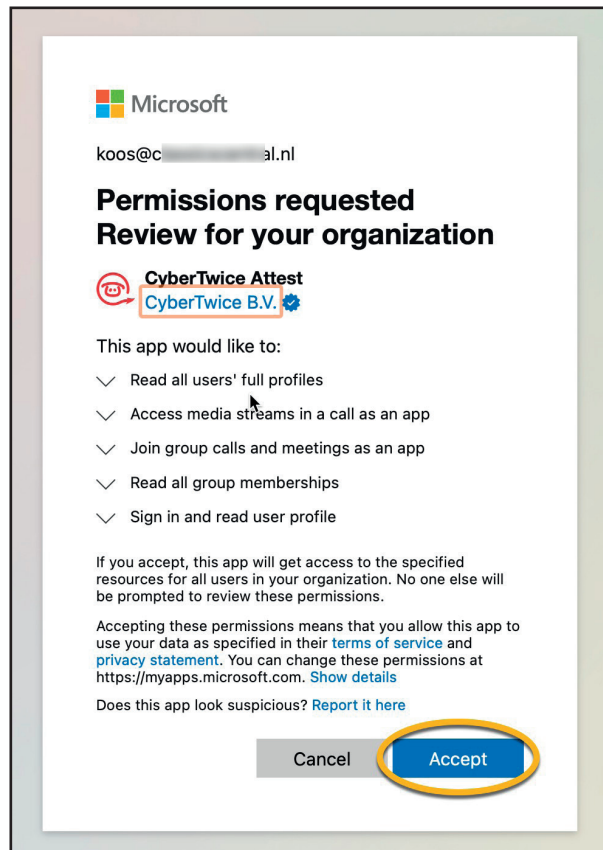
Before any recording related settings can be modified, consent has to be given to ATTEST.

- Click on the 'Consent tab' and click the 'Provide admin consent' button.



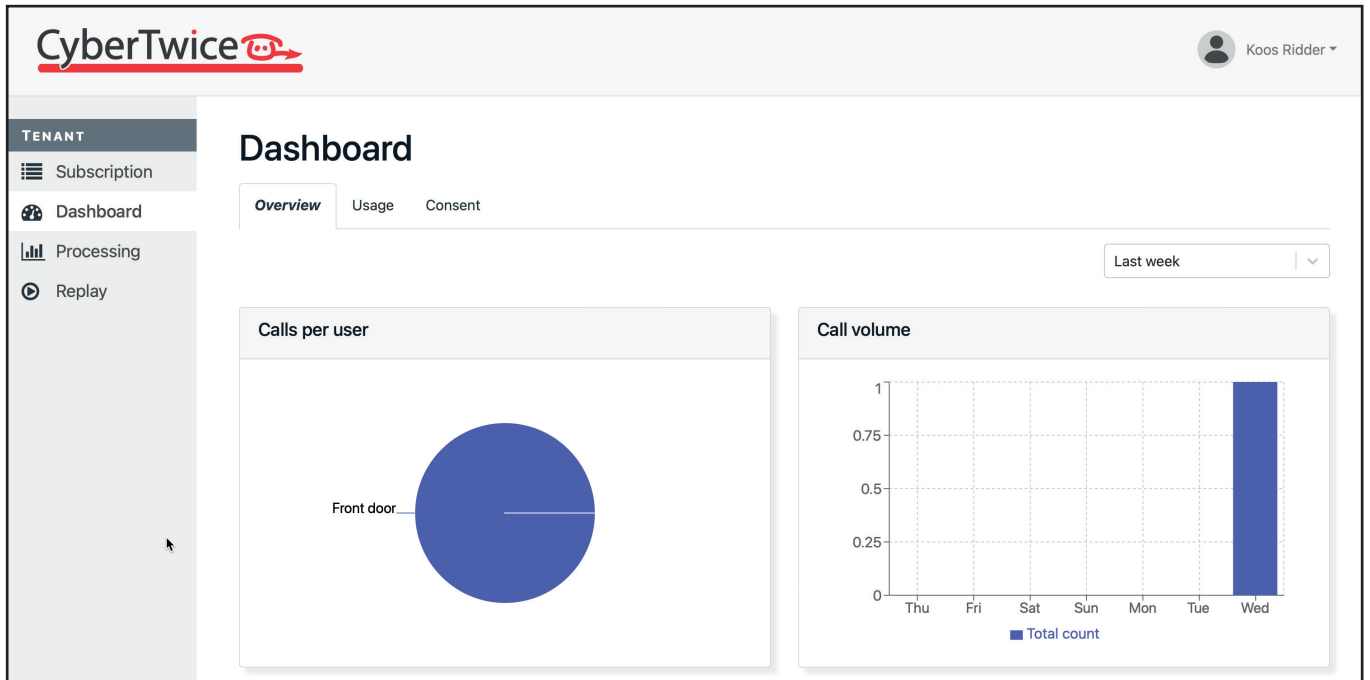
ATTEST management portal 'Dashboard' - 'Consent' tab

- Log in using a user account with **global administrator privileges** of your organization and accept the requested permissions



Microsofts 'Permissions requested' window

After consent has been given, the ATTEST management portal displays all features available.



ATTEST management portal 'Dashboard' - 'Overview' tab, consent given

By default, ATTEST Replay is only accessible for users with Administrator privileges. To allow non-Administrators in your Tenant to also access the recorded call in ATTEST Replay, navigate to the Replay option.

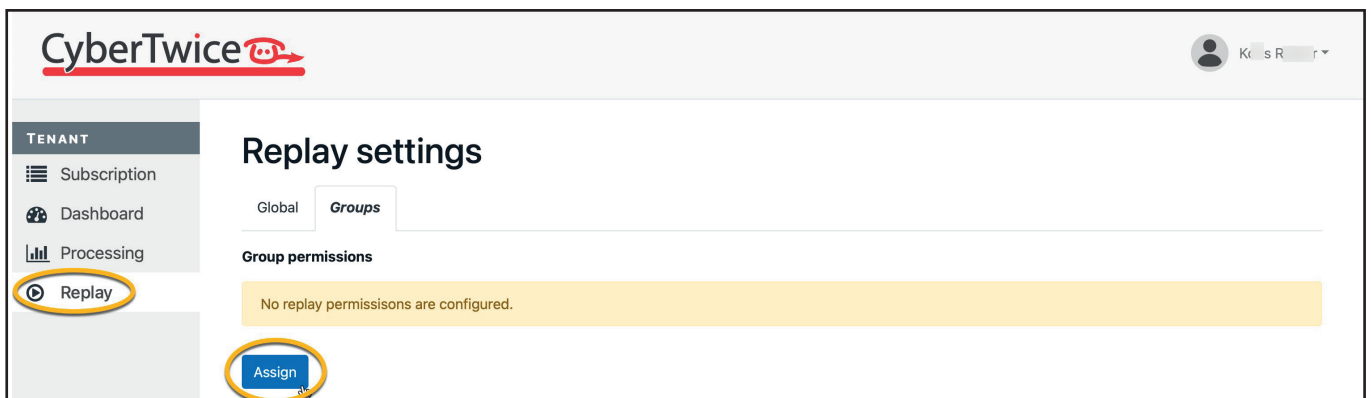
Allowing access to ATTEST Replay is done via groups, so people in an EntraID, M365 or Teams groups can be granted permission to access the call recordings.

Note:

it can take up to 30 minutes after Admin consent has been granted before group permissions can be set!



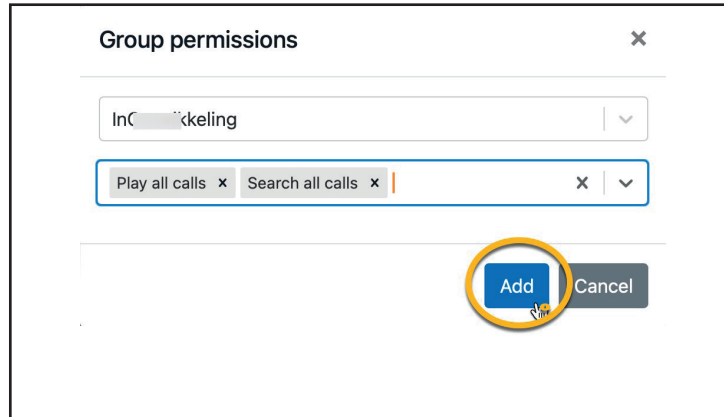
- Click on the 'Groups' tab to set group permissions.



ATTEST management portal 'Replay' - 'Groups' tab

In this example we are assigning a group with the two permissions 'Search own calls' and 'Play own calls'. This means that a user who is part of this specific group can search and play all calls.

- Click on 'Assign' to assign replay access rights to a specific group



ATTEST management portal 'Group permissions' - Assign permissions to a specific group

| Groupname | Id | Type | Permissions |
|--------------|--------------------------------------|------|--|
| InC...keling | fe7612c2-497d-47b3-b60f-1a91f7cc1c91 | Team | <ul style="list-style-type: none"> Play all calls Search all calls |

ATTEST management portal 'Replay' - 'Groups' tab, permissions assigned

Note:

To be able to view calls, select at least one of the two 'Search' permissions. If only Play permissions are set, no calls will be visible in the ATTEST Replay site.



Appendix D: Network requirements

As CyberGate is a SaaS (Software as a Service) solution, the SIP traffic and RTP (audio / video) coming from SIP devices like intercoms, cameras and pagers is directed to CyberGate.

Most networks are equipped with firewalls. To make sure CyberGate functions without issues, configuration of the locally used firewalls is essential. This Appendix covers the most important connection settings.

Outbound port configuration

Devices connecting to CyberGate are creating outbound traffic. Therefore the following ports need to be opened on firewalls:

| Port(s) / Protocol | Direction | Destination | Reason |
|---------------------|-----------|--------------------------|---|
| 5060 / TCP | Outbound | cybergate.cybertwice.com | SIP messaging |
| 5061 / TCP | Outbound | cybergate.cybertwice.com | SIP - TLS messaging (secure SIP) |
| 30000 - 30199 / UDP | Outbound | cybergate.cybertwice.com | (S)RTP ports (containing audio and video) |

Note:

Use the DNS name *cybergate.cybertwice.com* as the destination address. Do **not** use the resolved IP addresses as they will change without notice!



SIP ALG

A setting that can cause connection issues to CyberGate is the so called SIP ALG (SIP Application Layer Gateway).

SIP ALG is often enabled by default on firewalls. Although this feature should improve SIP messaging in theory, in practice it almost always does the opposite.

It is recommend to disable SIP ALG on the firewall for the devices that connect to CyberGate to prevent connectivity issues.

D

Communication Test Script

To test connections to CyberGate a Communication Test Script is available on the CyberGate management portal (admin.cybergate.cybertwice.com).

This Communication Test Script is a PowerShell script that will test all communication paths to CyberGate. The output of the script will show the outcome of the different tests.

In case of connection issues, download and run this Communication Test Script first.

Document History

| Document Version | Date | Author | Change |
|------------------|------------|--------|---|
| 1.0.0 | 14-07-2020 | KR | Initial version |
| 1.1.0 | 28-09-2021 | KR | Revised text and layout |
| 1.2.0 | 16-05-2022 | KR | Overhaul document (links, screenshots etc.) |
| 1.3.0 | 14-03-2023 | KR | Major overhaul (screenshots / descriptions) |
| 1.4.0 | 28-12-2023 | KR | Major overhaul (screenshots / descriptions) |
| 1.4.1 | 03-01-2024 | KR | Added chapter |
| 1.4.2 | 06-08-2024 | KR | Updated screenshots and descriptions |
| 1.4.3 | 13-09-2024 | KR | Added Appendix D: Network requirements |
| 1.4.4 | 06-12-2024 | KR | Added 2 and 3 year purchase options |
| 1.5.0 | 16-04-2025 | KR | Major overhaul (screenshots / descriptions) |
| 1.5.1 | 17-11-2025 | KR | Microsoft Marketplace implementation |