CyberTwice

# 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

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

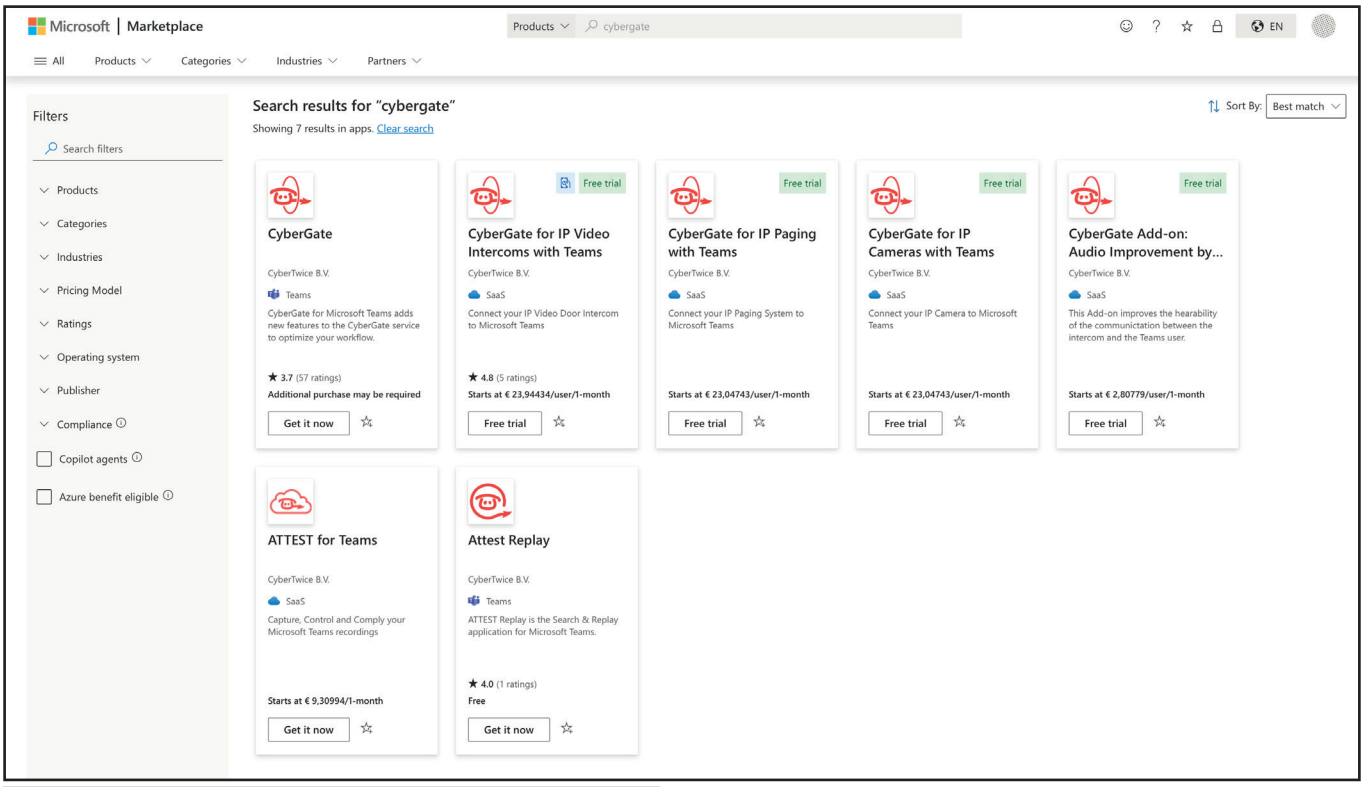
Follow the instructions below to purchase CyberGate in Microsoft Marketplace.

***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

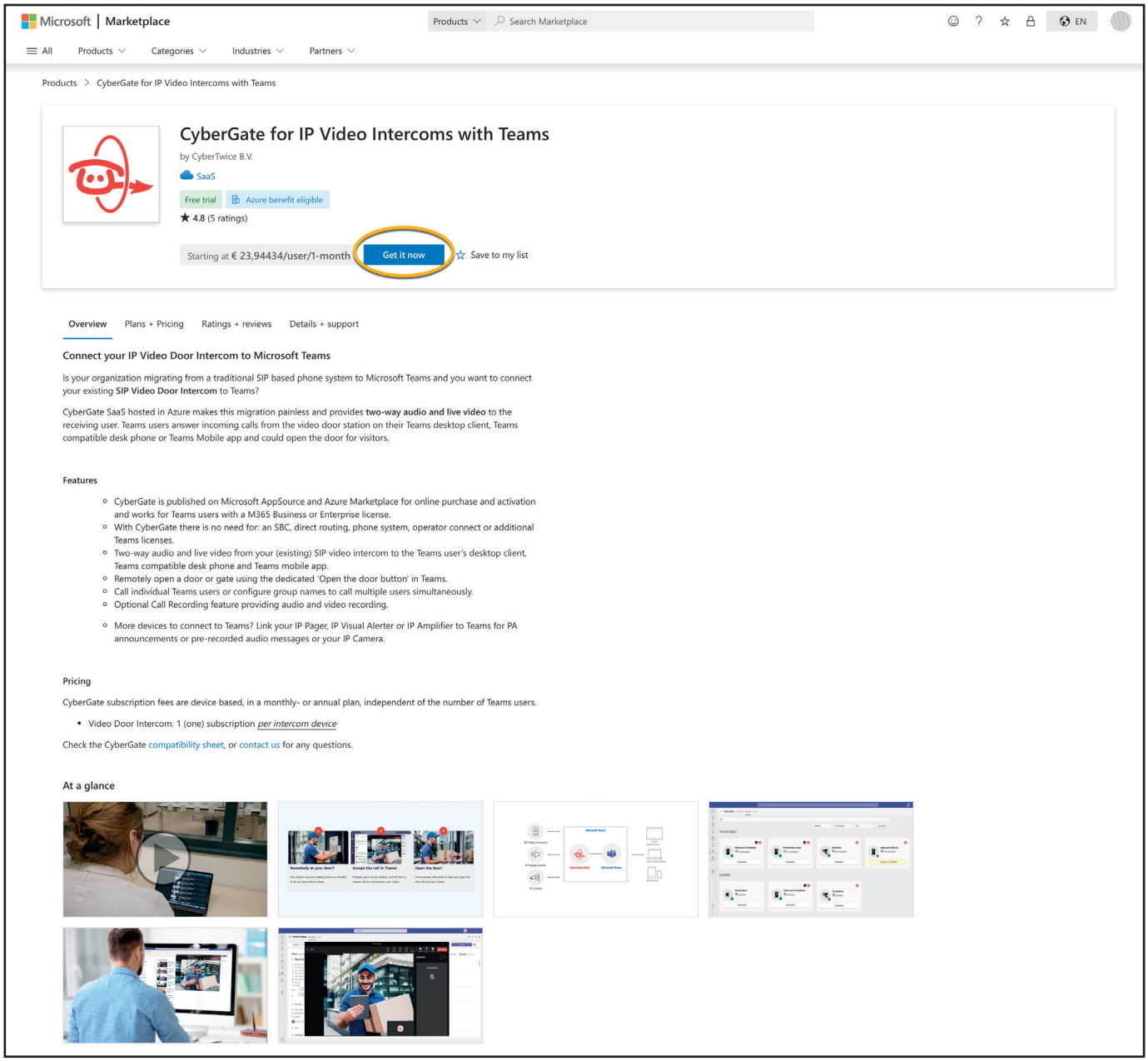



*Marketplace and the search result for 'cybergate'*

- Click on 'Free trial' to start the purchasing procedure

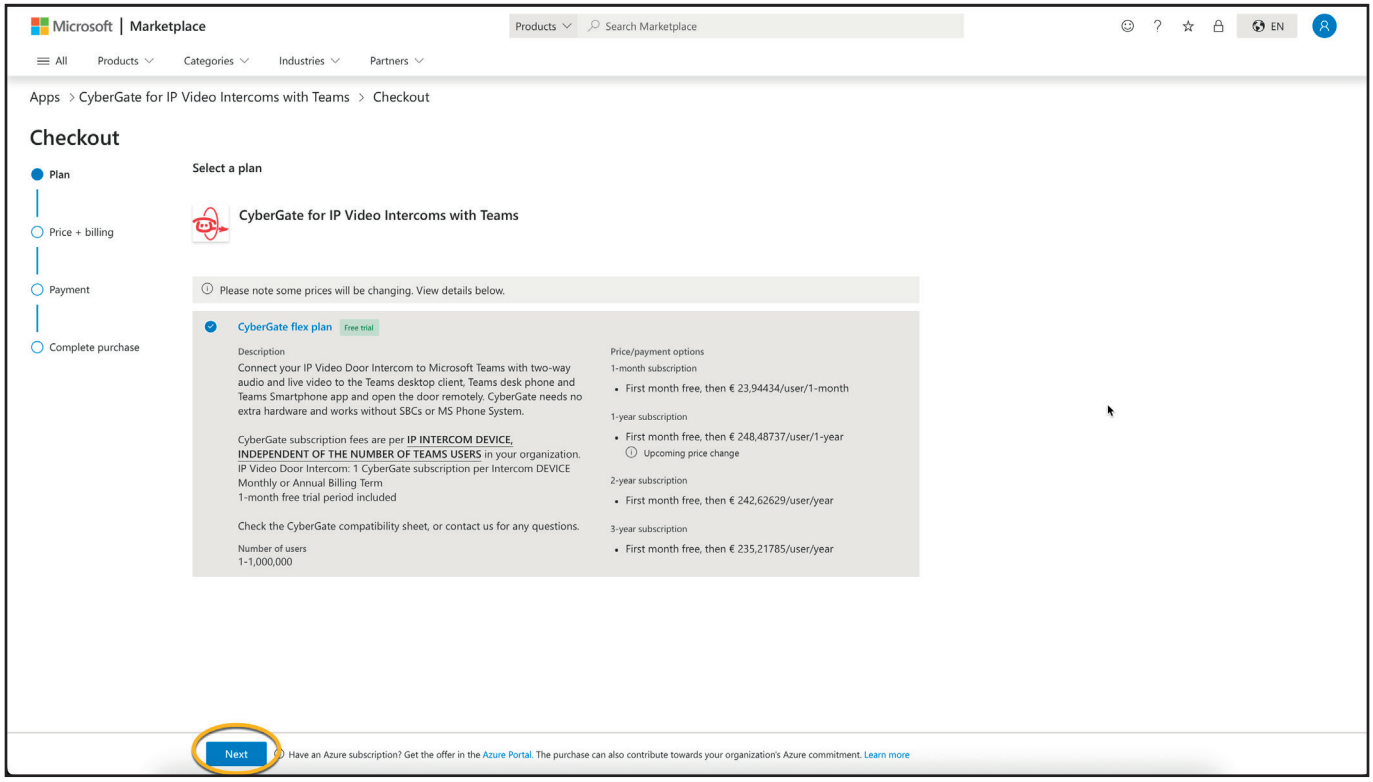
The overview page provides information regarding CyberGate, plans, pricing information and reviews.

- Click ‘Get it now’ to start the purchasing procedure




*CyberGate ‘Overview’*

- Select the CyberGate flex plan and click 'Next'




*CyberGate 'Plan'*

- Select the billing term.
- For pricing check the CyberGate pricing page (*Link*)

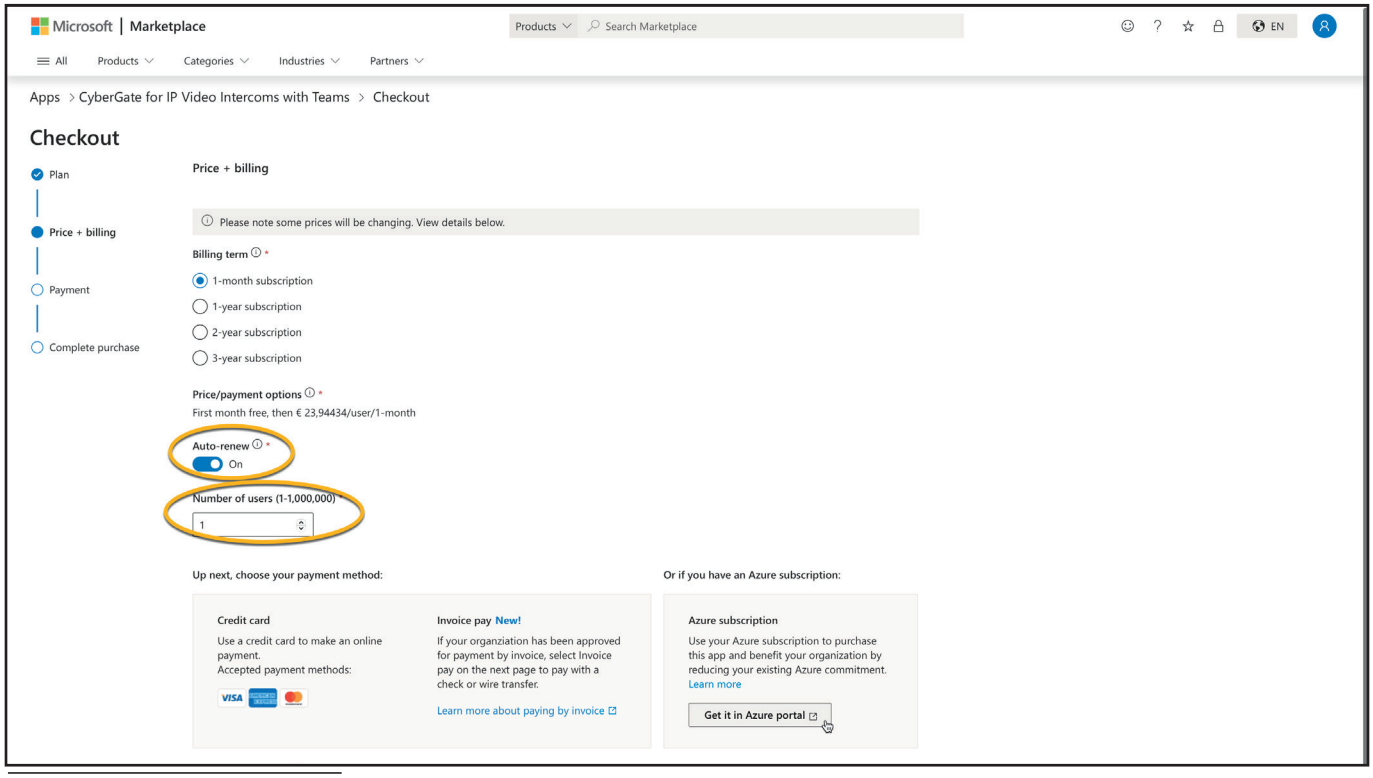
*Note:*
*All CyberGate Billing Terms come with a 30 day free trial period.*

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.

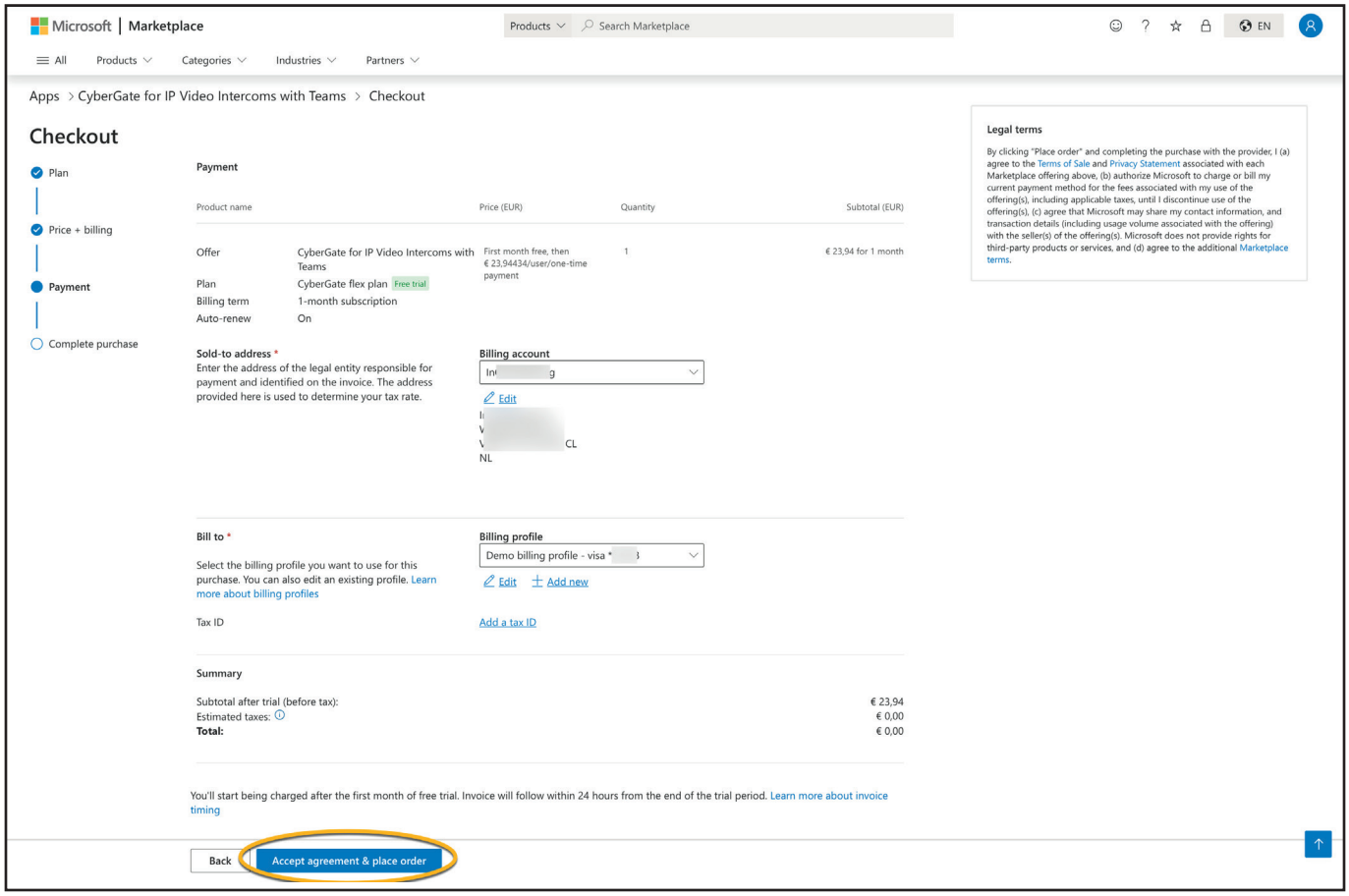
***Note:***
***Payment via Azure? "Purchase in Microsoft Azure" on page 14 for instructions how to continue purchase CyberGate***

- When done, click 'Next'



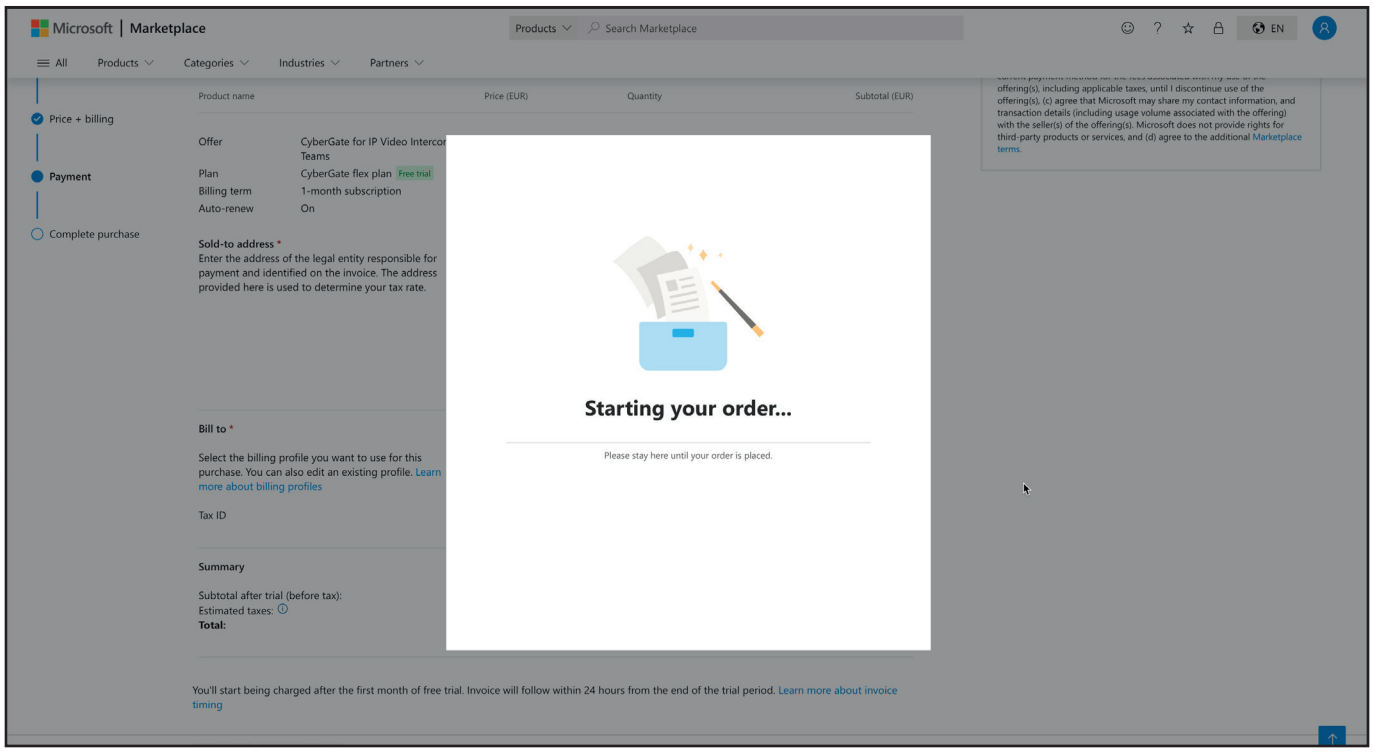

*CyberGate price + billing*

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




*CyberGate complete purchase*

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

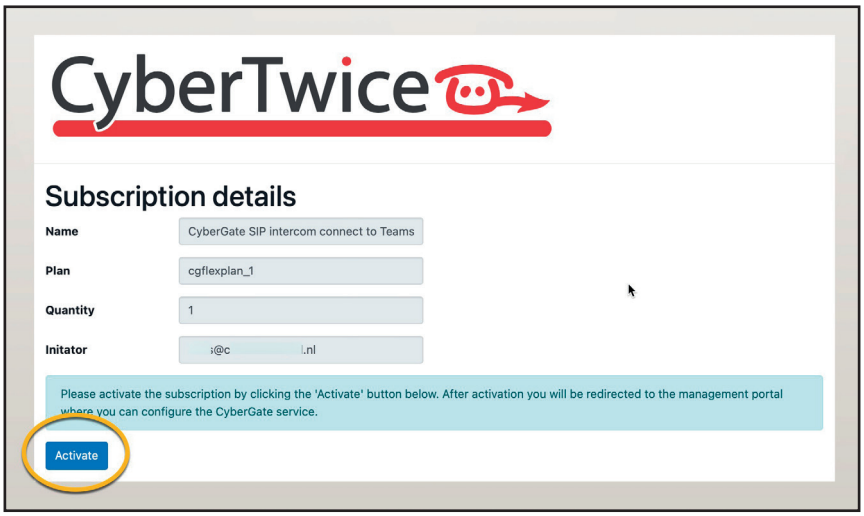



*CyberGate purchasing in progress*

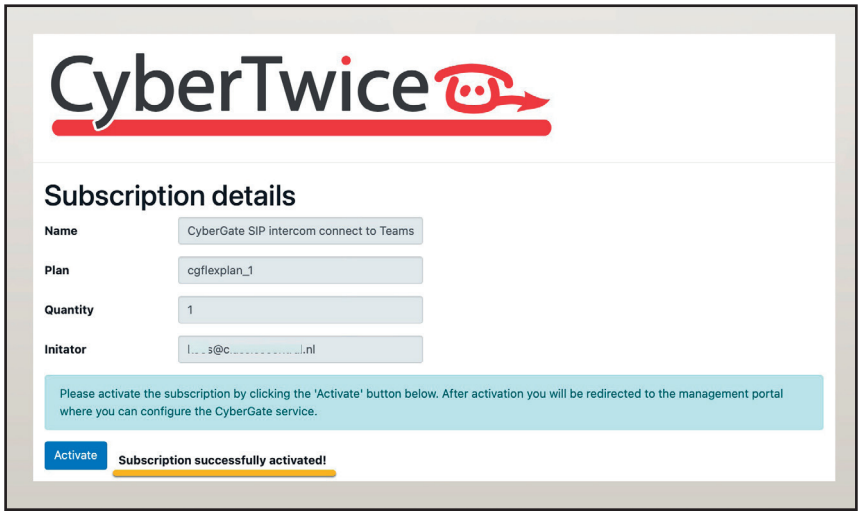
The Microsoft Marketplace will redirect you to the CyberGate Management Portal where you can activate your CyberGate Purchase.

*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.

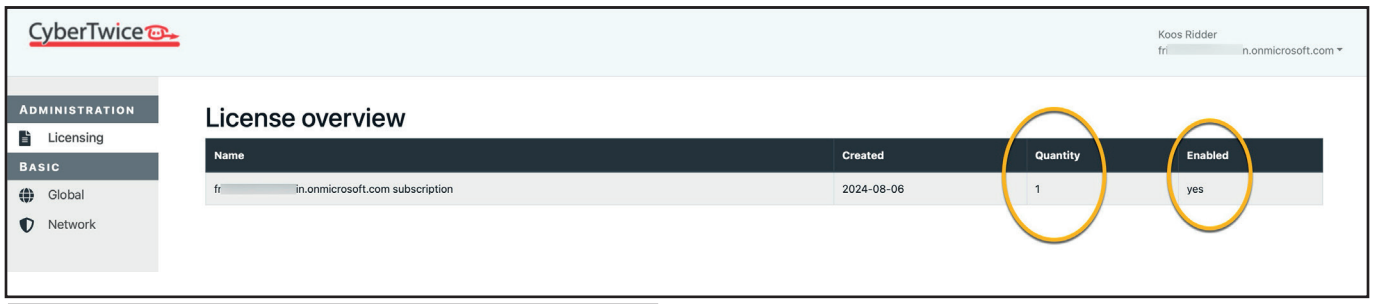



*CyberGate overview of the 'Subscription details'*




*CyberGate successfully activated*

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




*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***

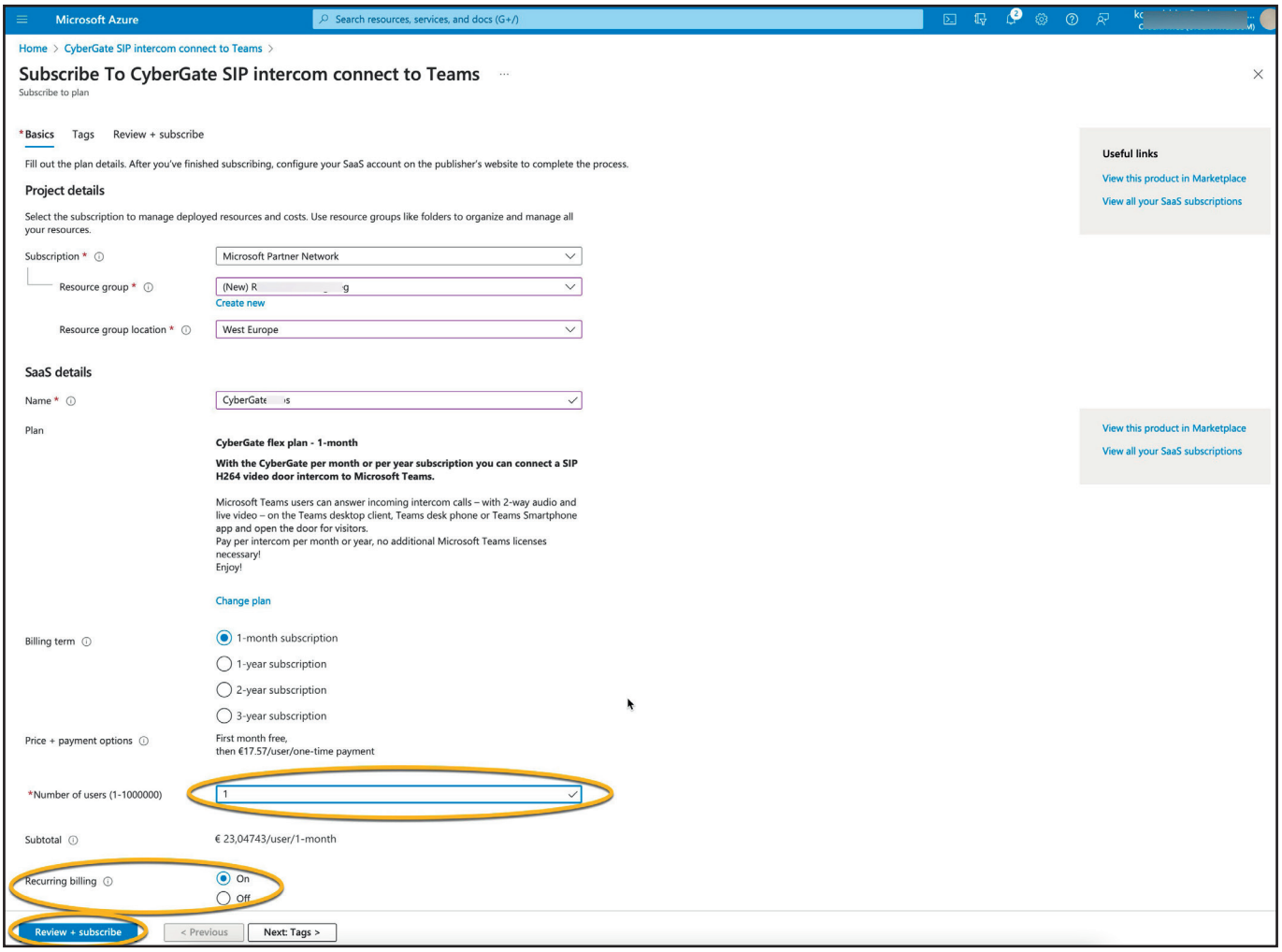
In Azure, the CyberGate offer will be opened automatically.

- 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.*

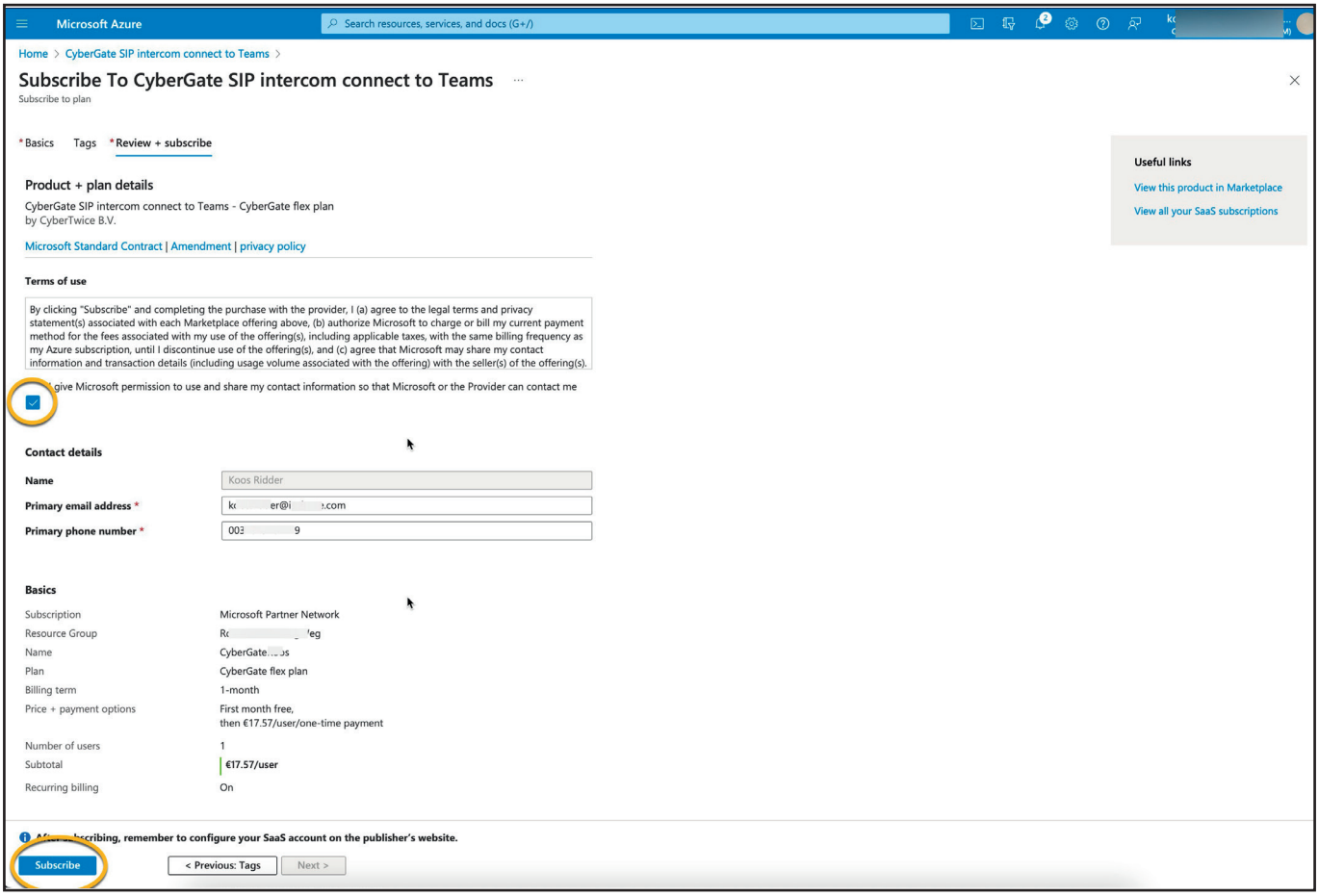
You can have one subscription to CyberGate and use multiple devices on that subscription. The 'User count' can be read as the 'number of devices' used with this subscription. You can always modify the amount of devices on this subscription later on, in the CyberGate Management portal.

- 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'.

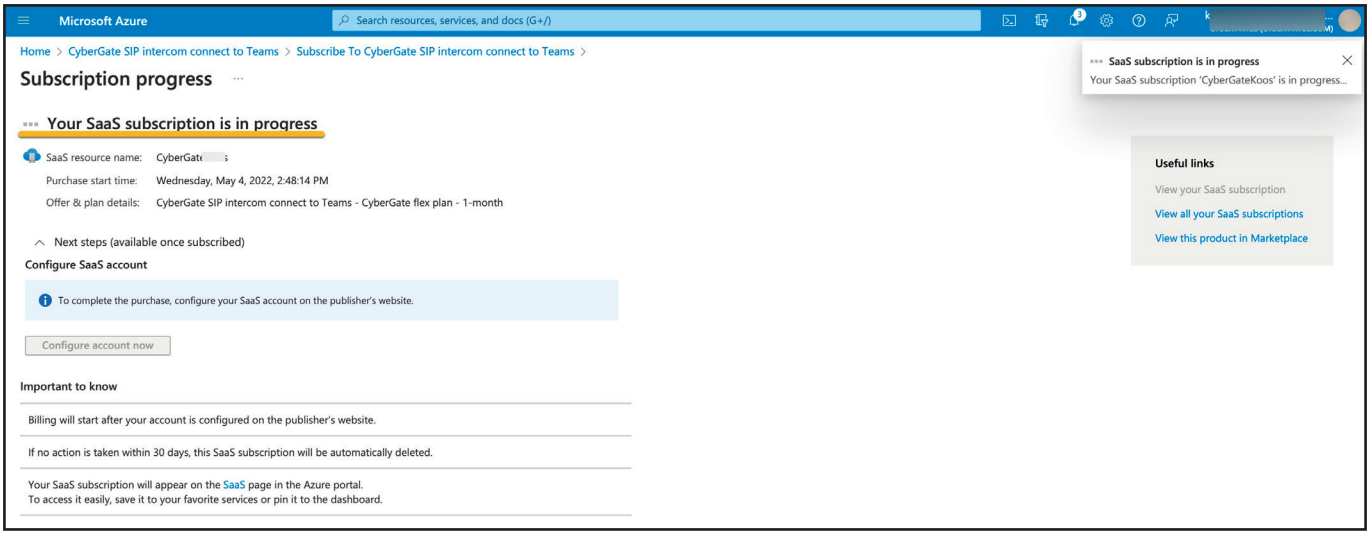



*Azure portal, CyberGate details*

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



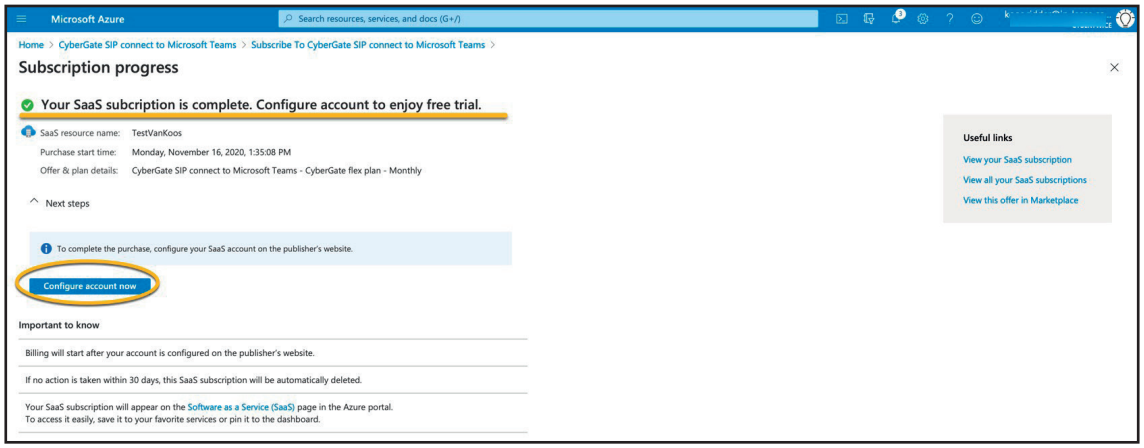

*Azure portal, CyberGate review*




*Azure portal, subscription is in progress*

Wait for the subscription to finish.

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

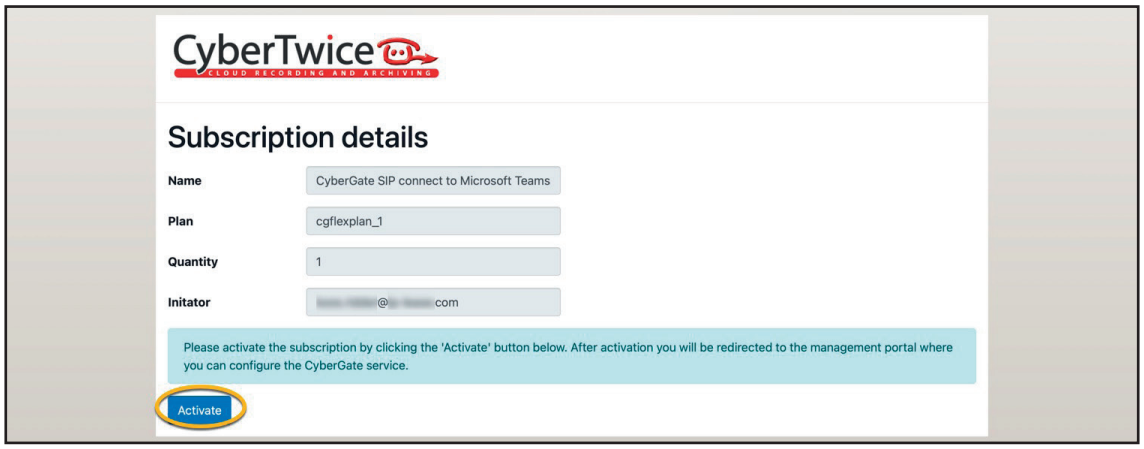



*SaaS subscription complete*

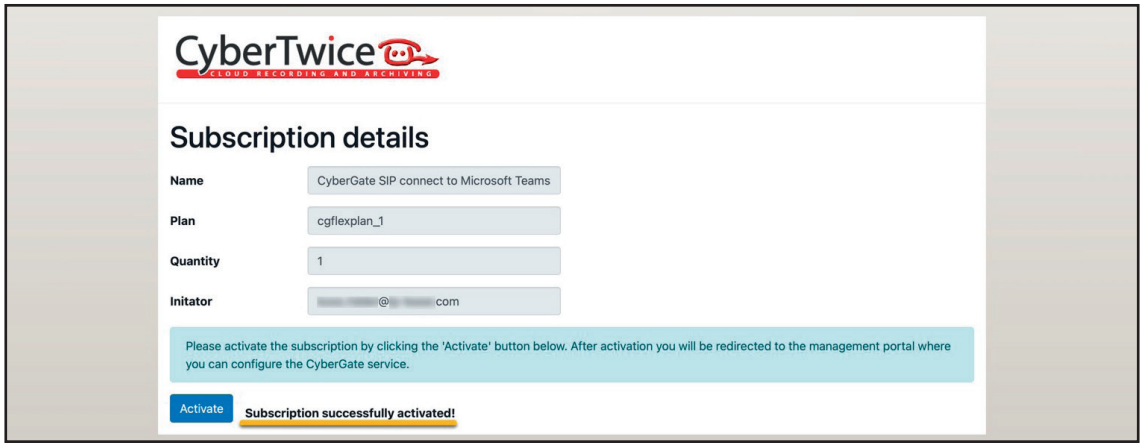
Azure Marketplace will redirect you to the CyberGate Management Portal where you can activate your CyberGate Purchase.

*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.

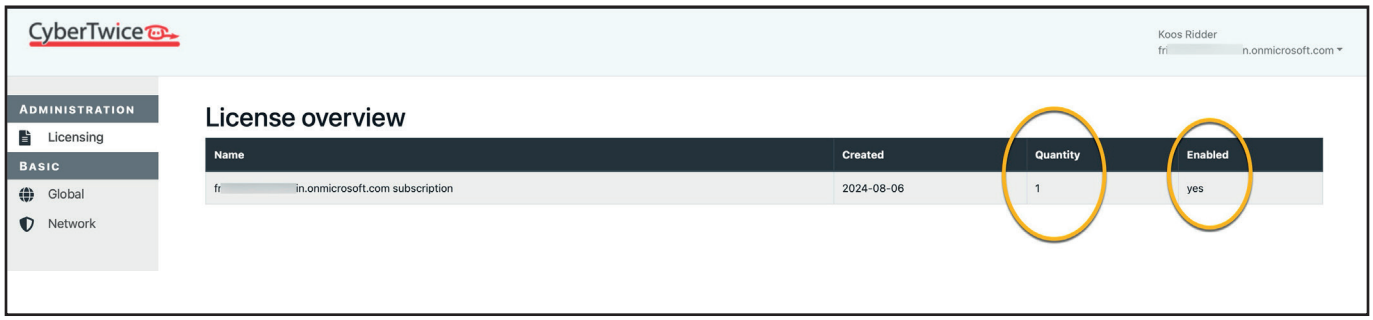



*CyberGate overview of the 'Subscription details'*




*CyberGate successfully activated*

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




*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**

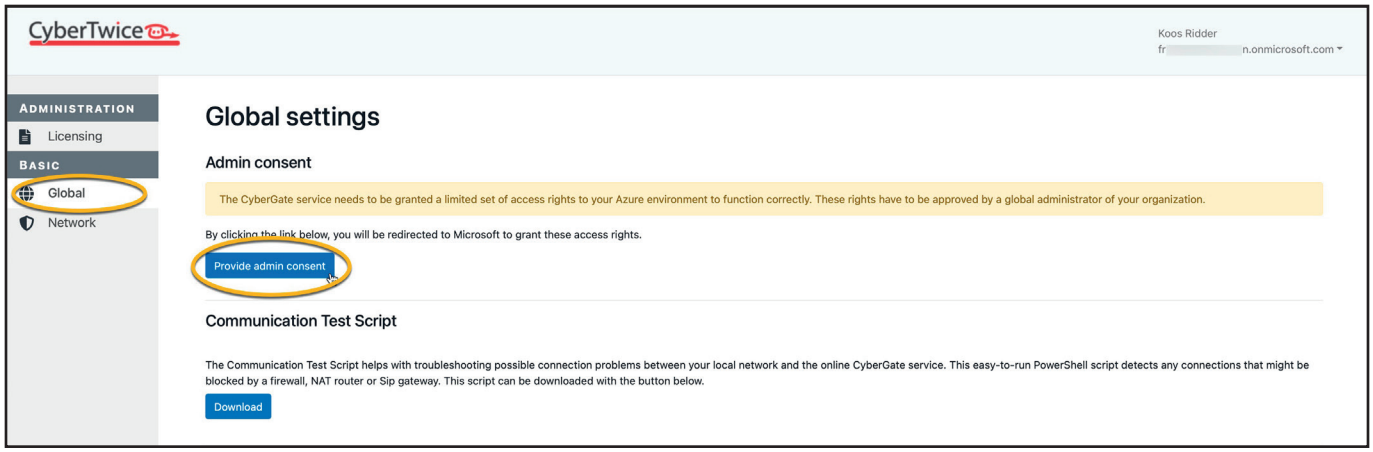
## Provide Admin Consent

*Global settings*

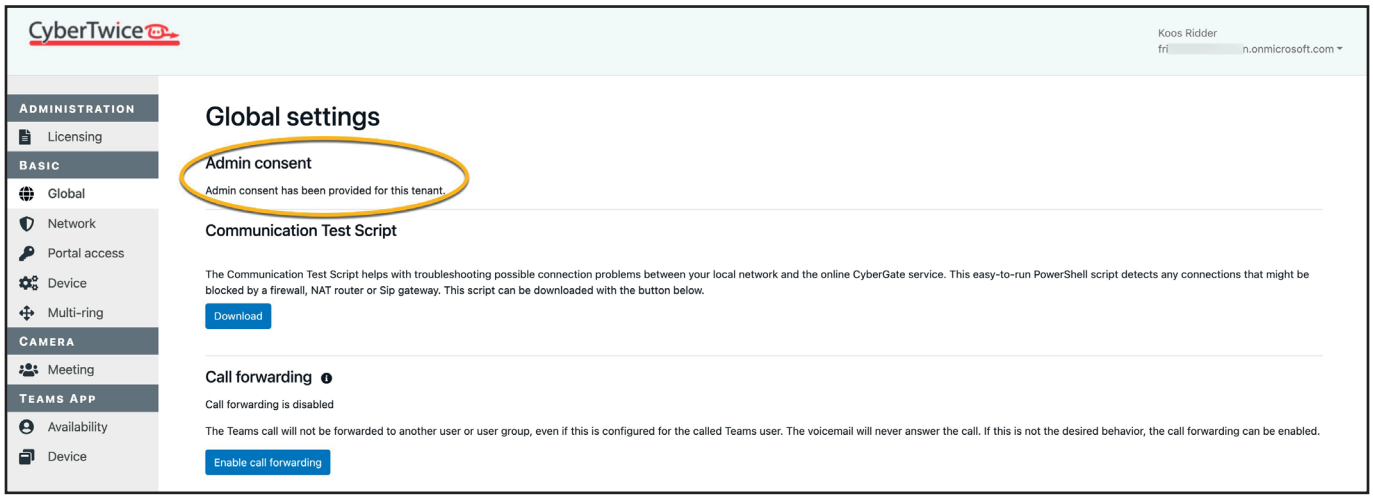
In the section '*Global*' you have to grant CyberGate limited access to your Azure environment. This is mandatory to be able to call Teams users in your organisation.

- 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!*




*CyberGate management portal 'Global' - Provide admin consent*




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

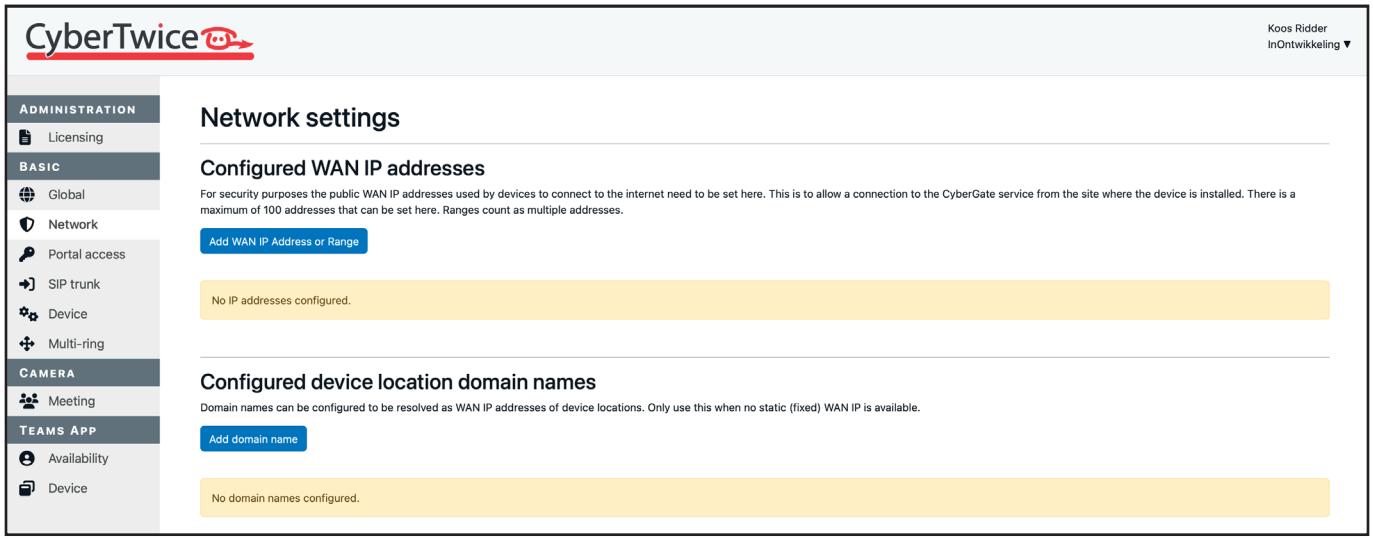
- Click -Basic-Network- for the next step'.

## Network settings

One of the security measures of CyberGate is a white list that containes 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.

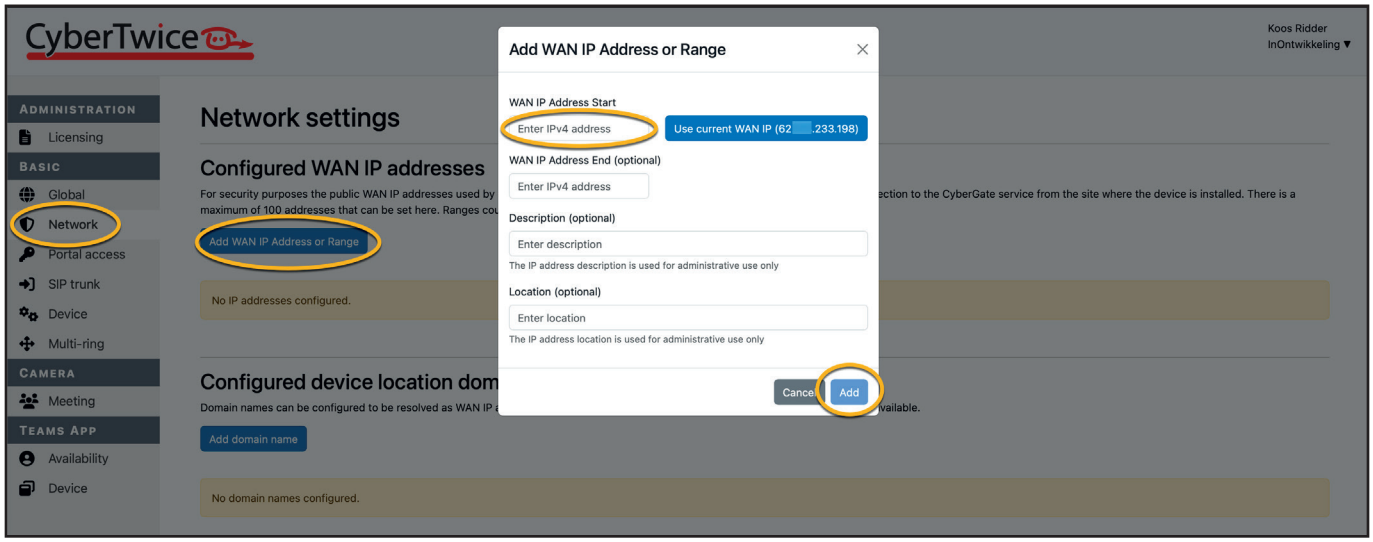
- Click ‘Add WAN IP Address or Range’

The setting is saved automatically.

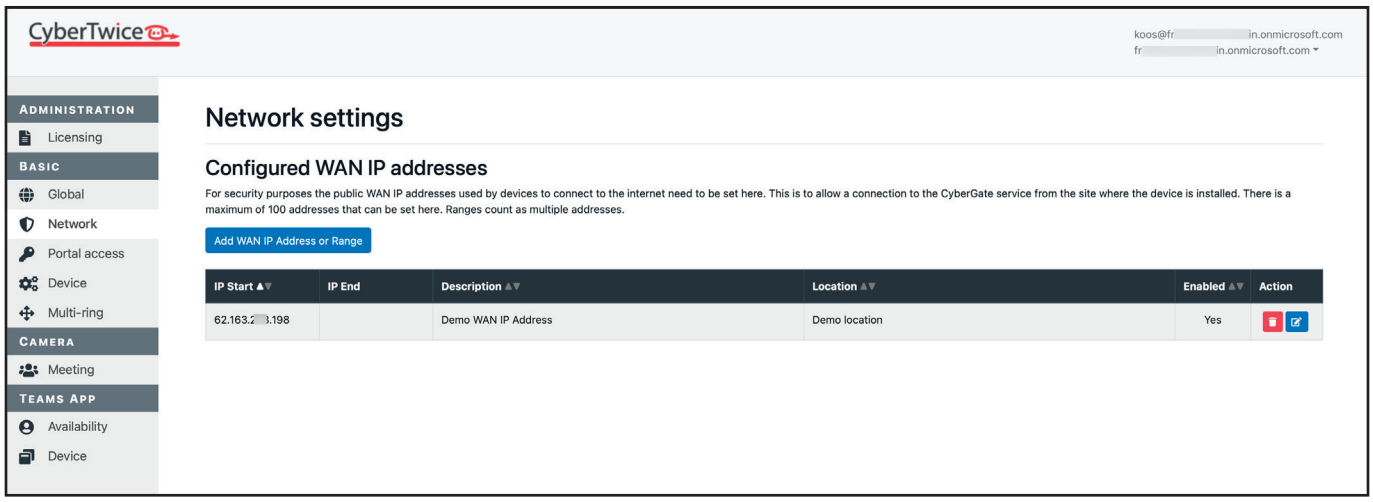



*CyberGate management portal ‘Network’ - No WAN IP address configured yet*

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




*CyberGate management portal ‘Network’ - Add WAN IP address or Range*




*CyberGate management portal 'Network' - WAN IP address configured*

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

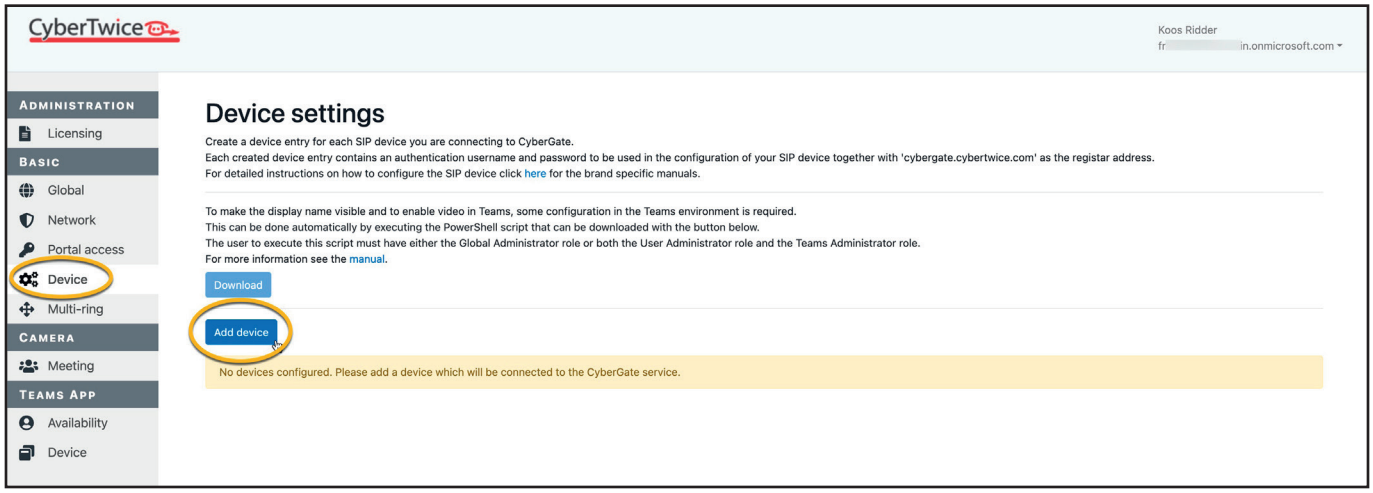
## Device settings

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.

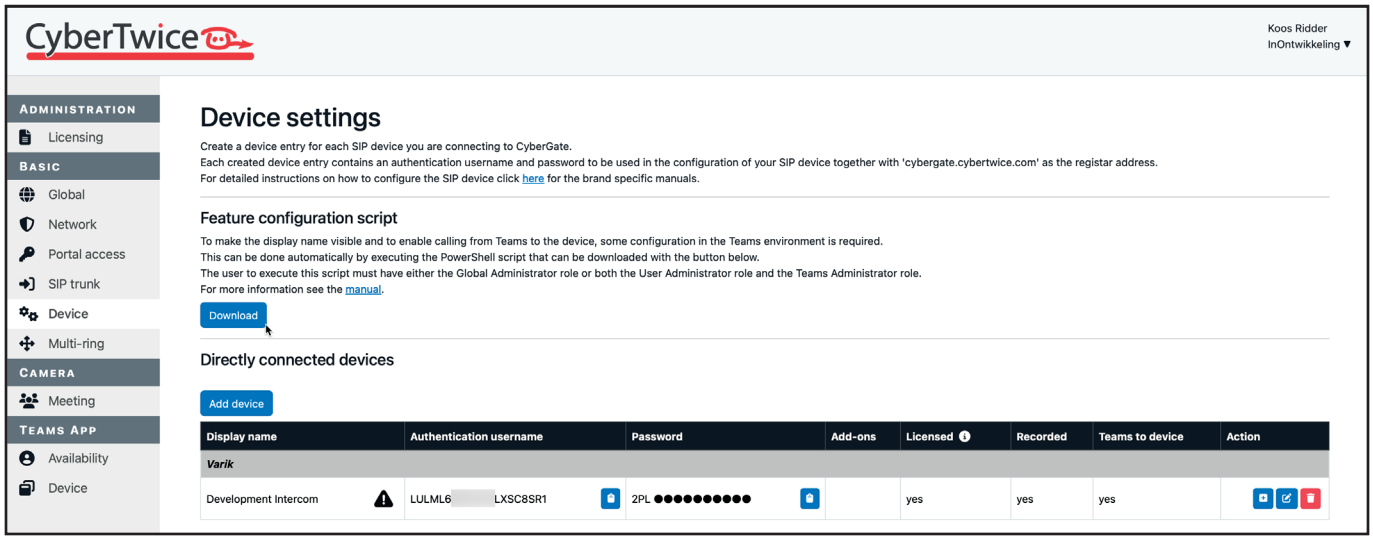
- Click 'Add device'

- Configure:
  - Display Name (a descriptive name for this device)
  - Type (Intercom, Pager of Camera)
  - Location (location of the device)

- Click 'Add' to add this device




*CyberGate management portal 'Device' - 'Add device'*




*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.

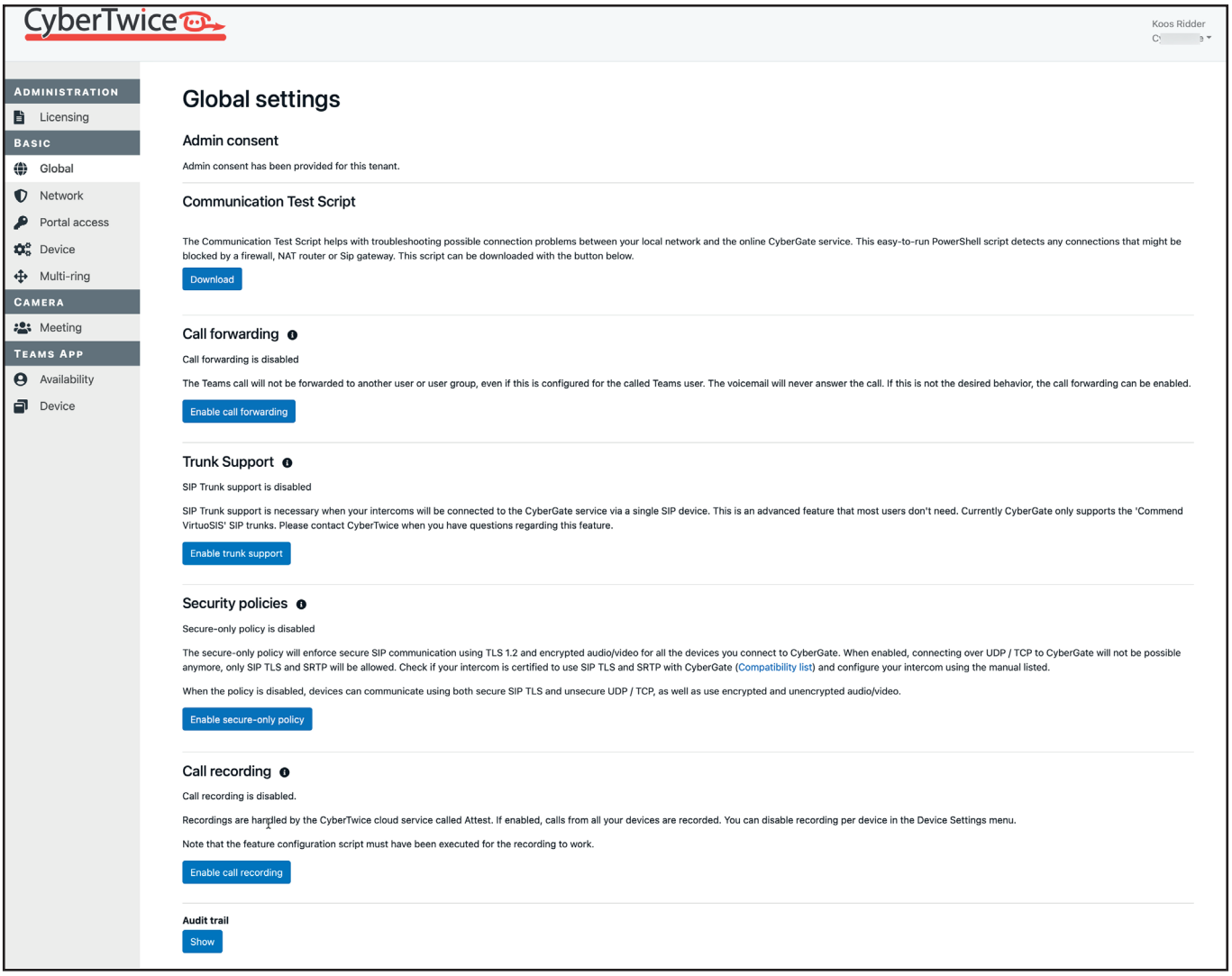
*Enabled*
If the CyberGate license is active and paid, the 'Enabled' status will show 'yes'. If it shows 'no', this subscription and the intercoms using this subscription will not work. In that case check the subscription in the Microsoft portal (*https://portal.microsoft.com*) for more details.

*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




*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.

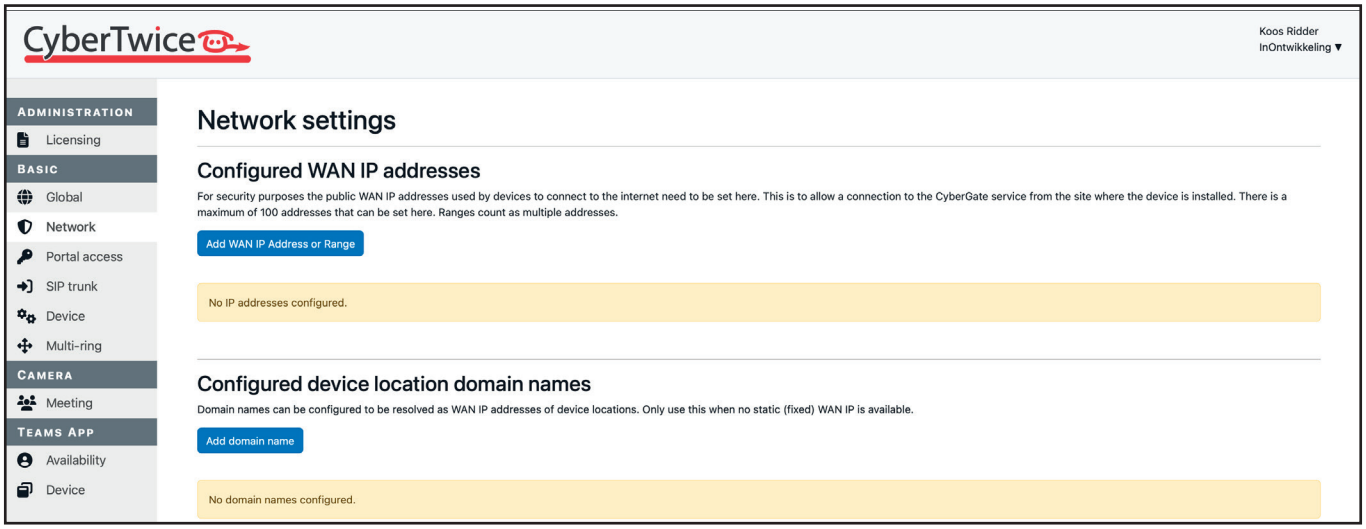
## Network

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

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

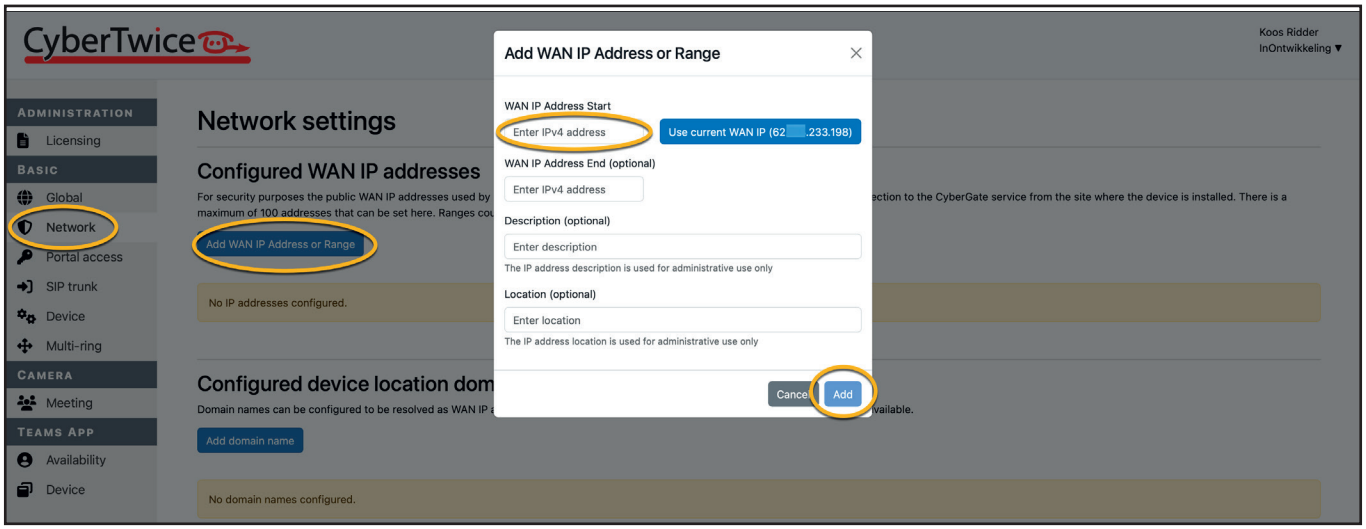
In order for a device to register with CyberGate, the public WAN IP-address your intercom is using to connect to CyberGate has to be configured in the Basic-Network menu.

> *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.*



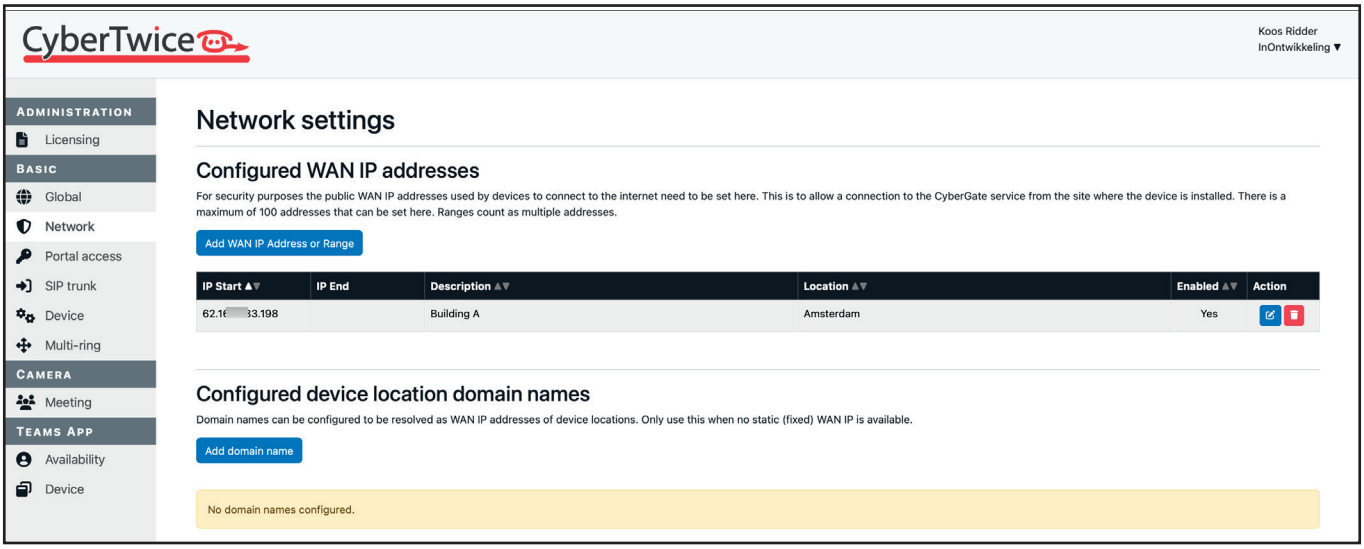

*CyberGate management portal 'Network' - 'Nothing configured'*

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




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

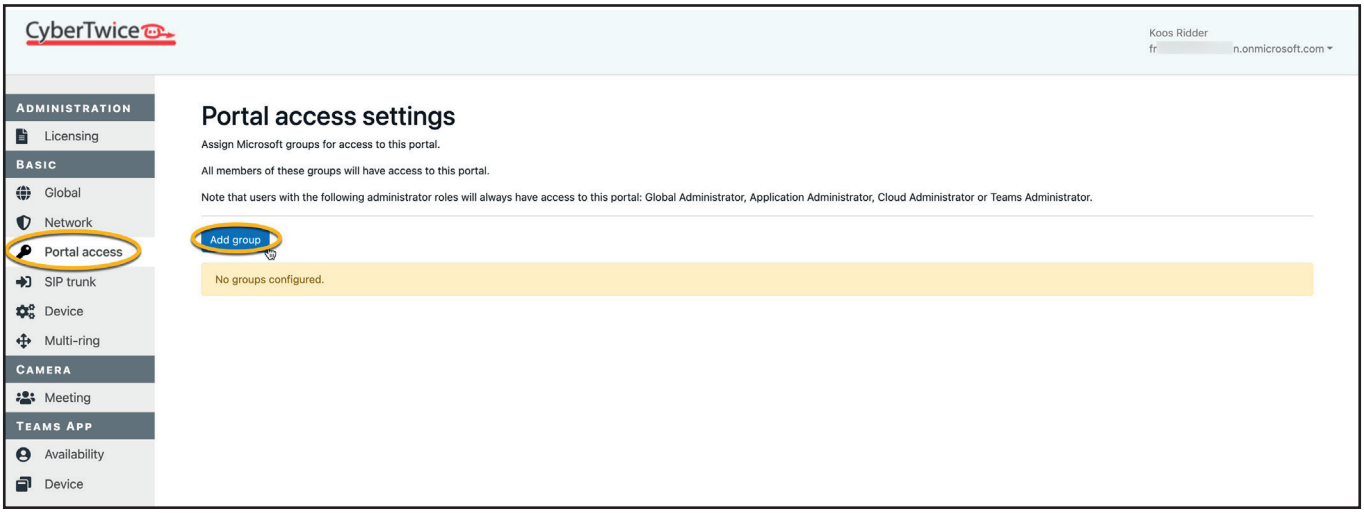
- Add the WAN IP address (optional: define a range of addresses)
- Add an optional description and / or location




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

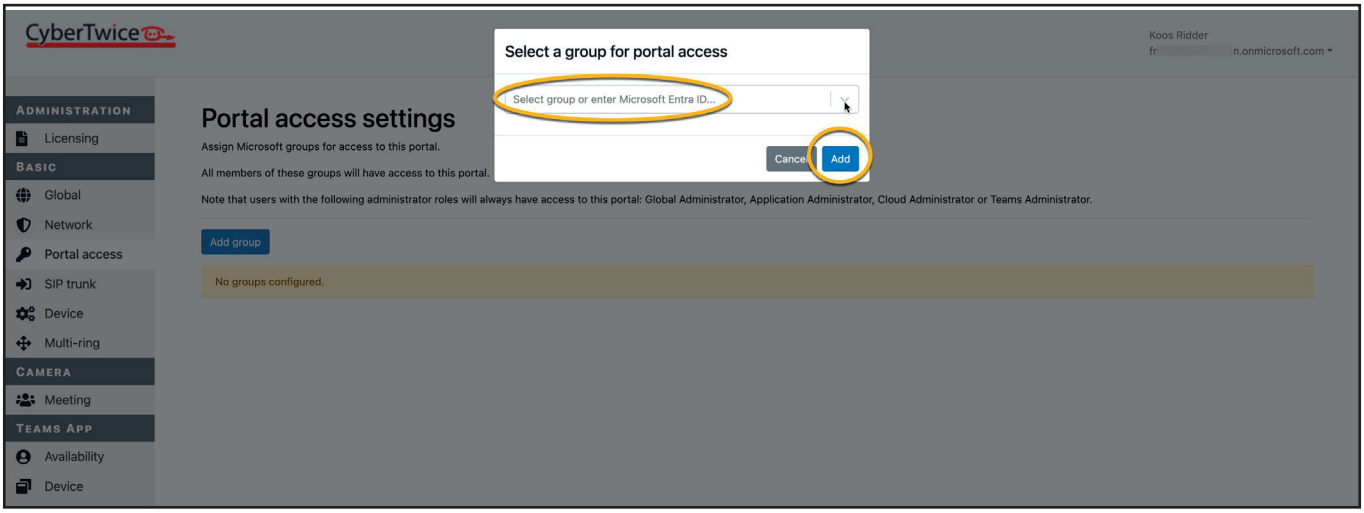
## Portal access

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.



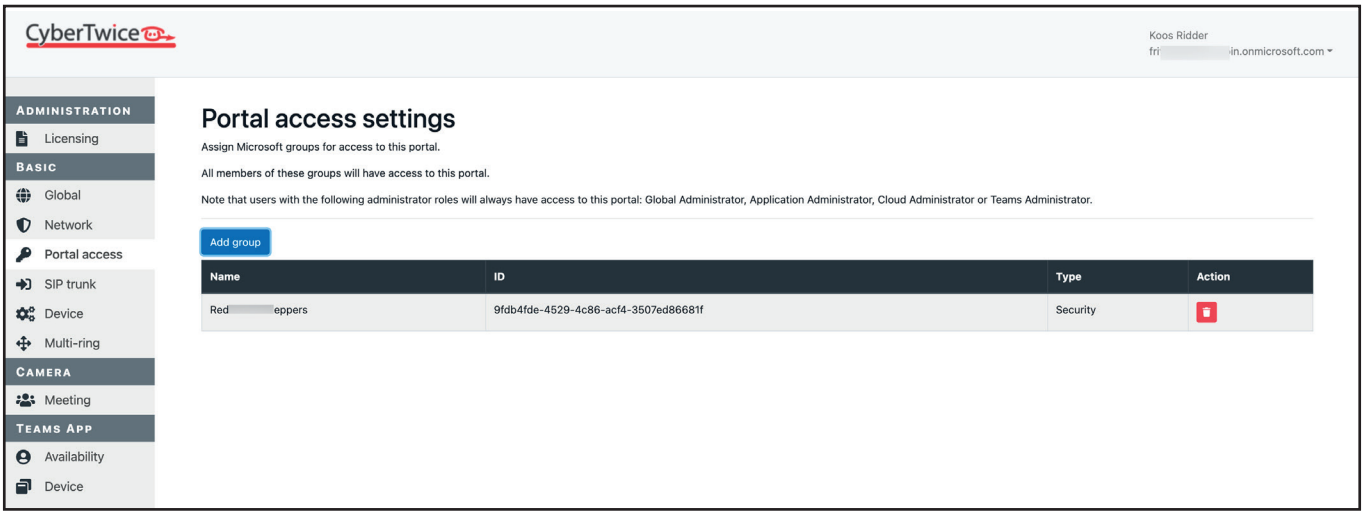

*CyberGate management portal 'Portal access' - 'No group added yet'*

- 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.



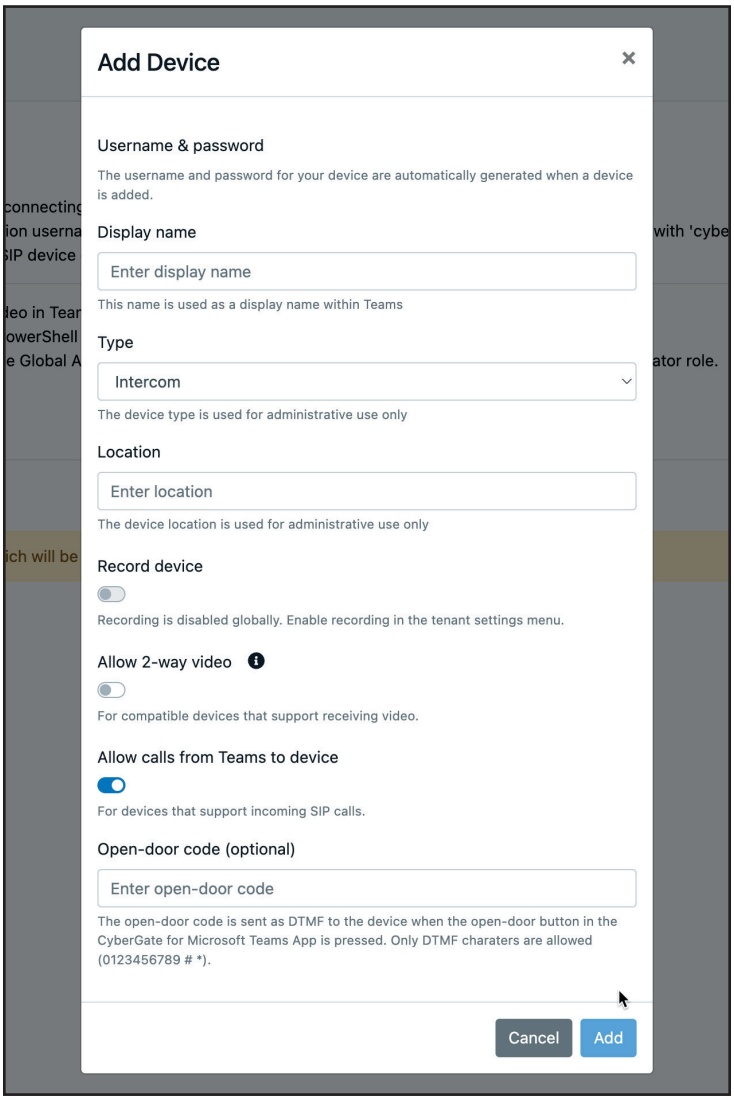

*CyberGate management portal ‘Portal access’ - ‘Group added’*

## 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.




*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.

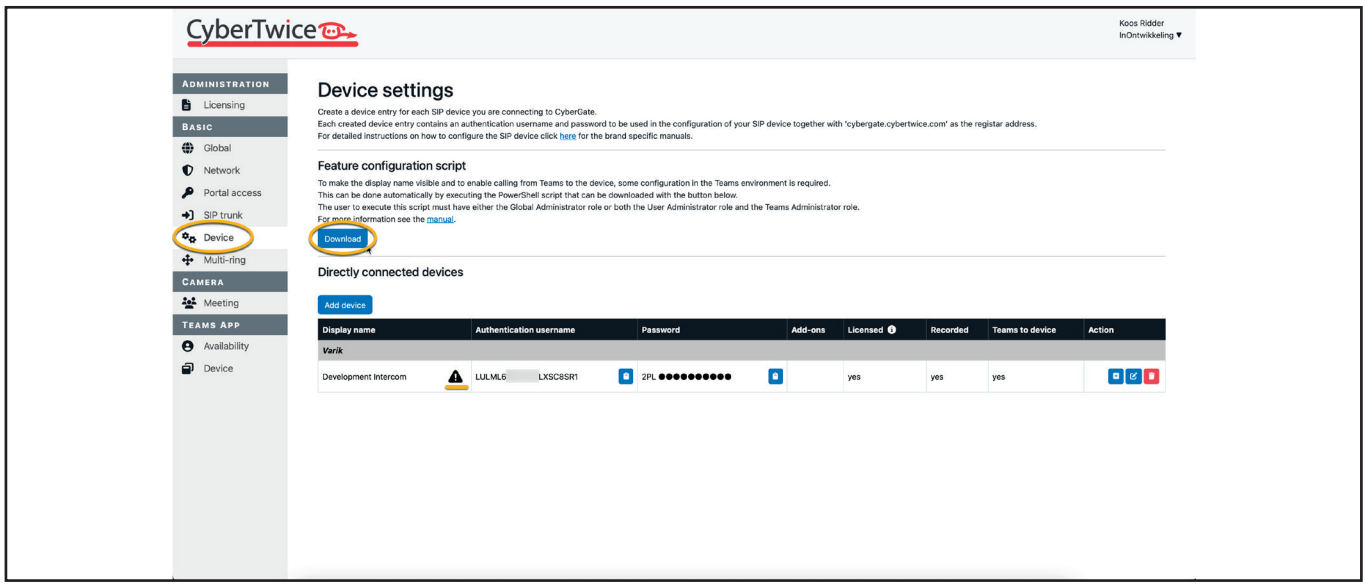
*Note:*
*Refer to the Appendix B: Configure the display name of the device for instructions on how to modify the display name from the default 'Intercom' to the Display name given.*

*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.*




*CyberGate management portal 'Device' - 'Device added'*

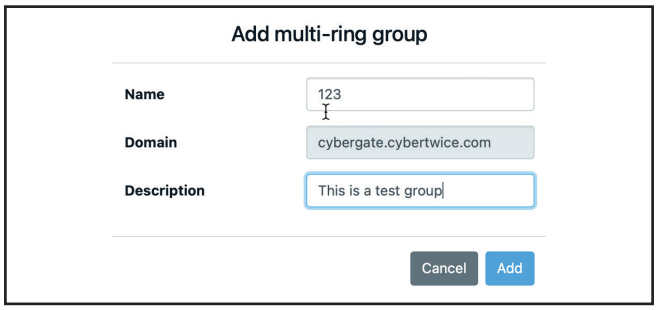
*Note:*
*If the Display name field will show the name and show an explanation mark symbol, the device will be able to call to Microsoft Teams, but will show the name 'Intercom' instead of the custom Display name until you execute the PowerShell script that can be downloaded on this page.*

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.



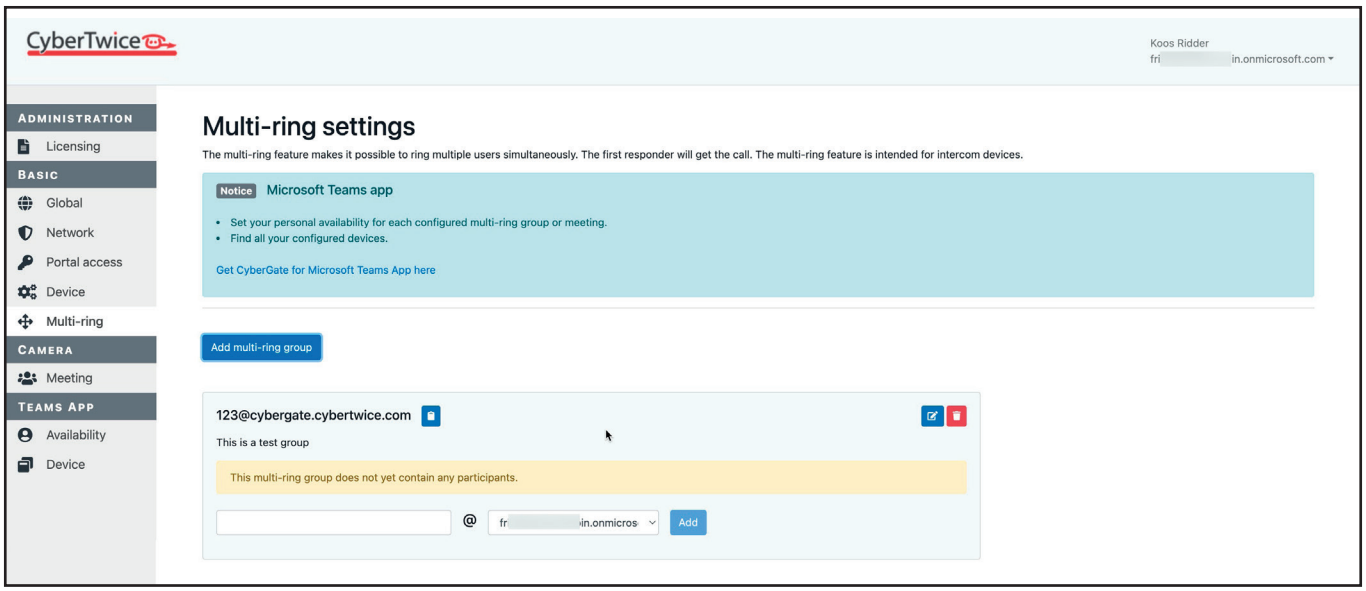

*CyberGate management portal 'Add multi-ring group'*

- Name the Multi-ring group and add a description

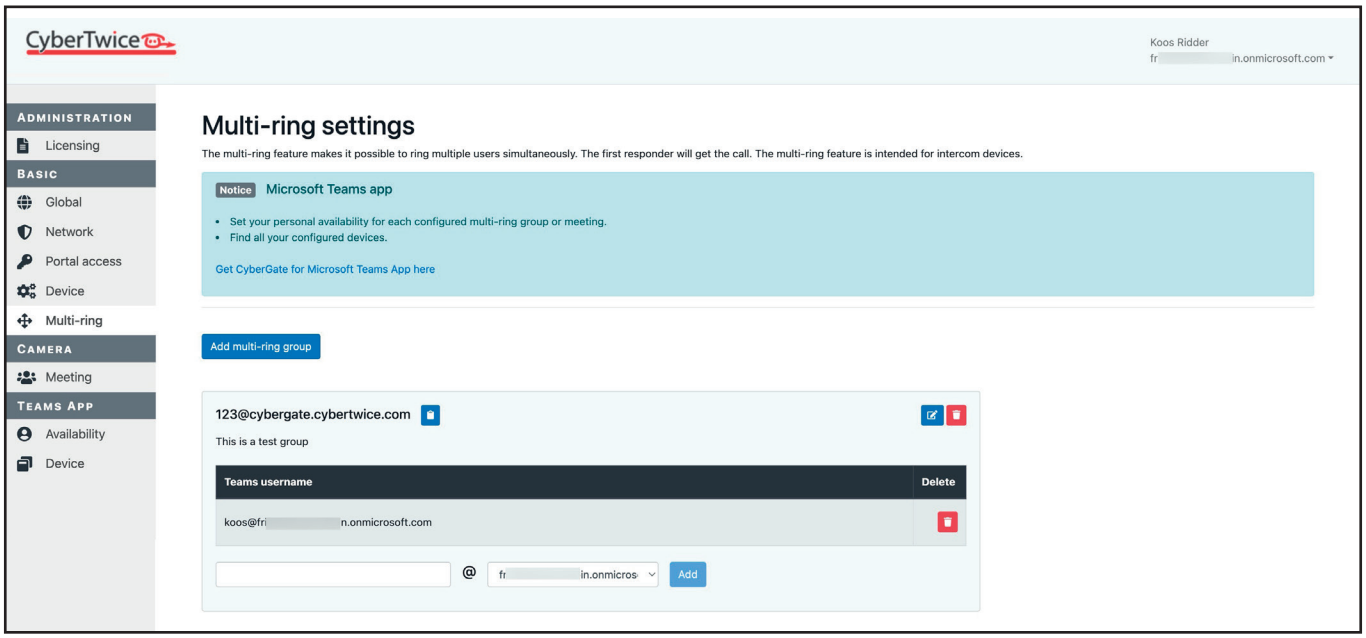
The name combined with the fixed domain: cybergate.cybertwice.com will make the call destination. E.g.: If the name is *123*, the name to dial in the intercom will be: *123@cybergate.cybertwice.com*.

*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.




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



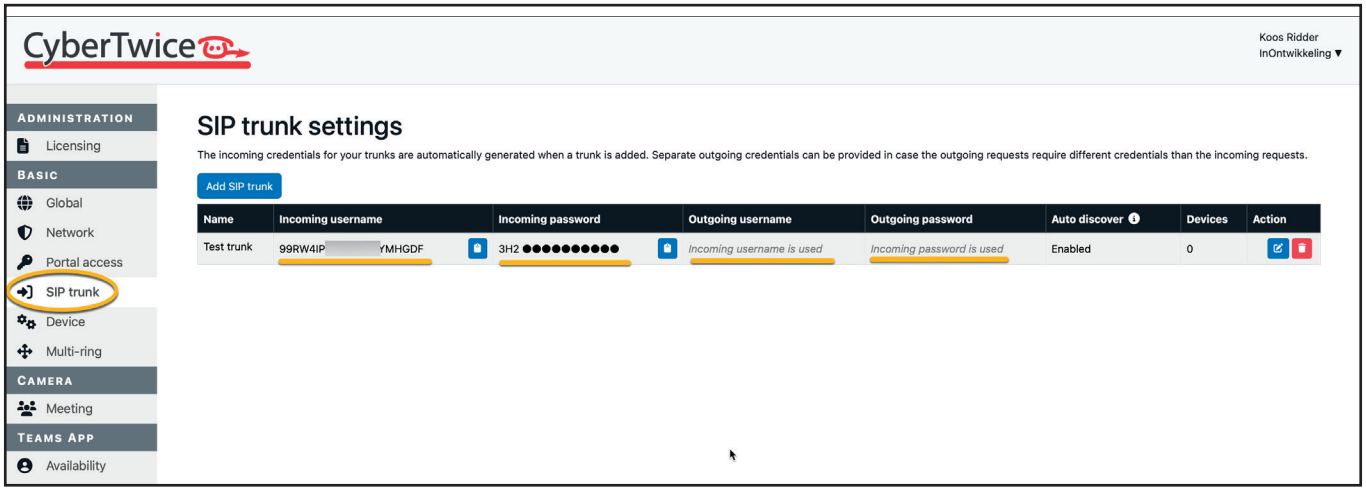

*CyberGate management portal 'Multi-ring' - 'User added to the Multi-ring group'*

## 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 Commend 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.




*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.*

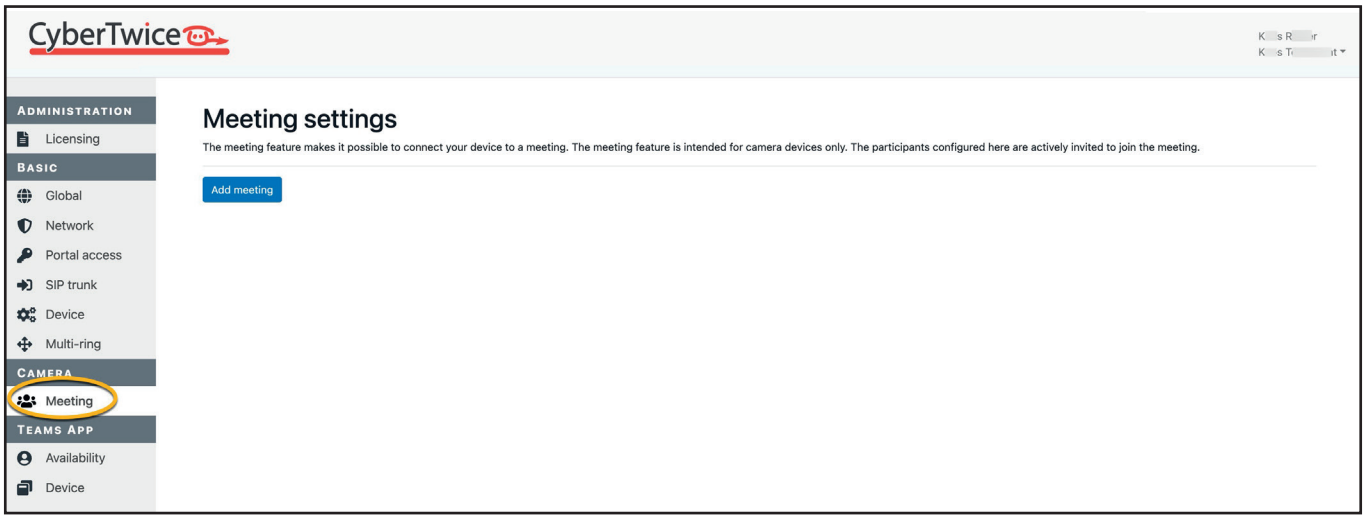
## Camera

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

### Meeting

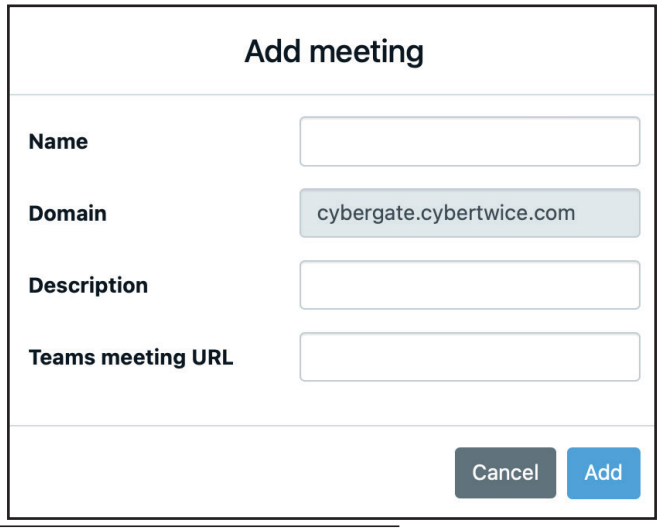
The meeting feature allows a device to join an existing meeting. If the device is configured to use the Meeting feature, it will automatically join a meeting instead of calling a Teams user. This meeting can than be joined by one or more Teams users to allow them all to access the audio and video of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




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

- Click 'Add meeting' to create a meeting.



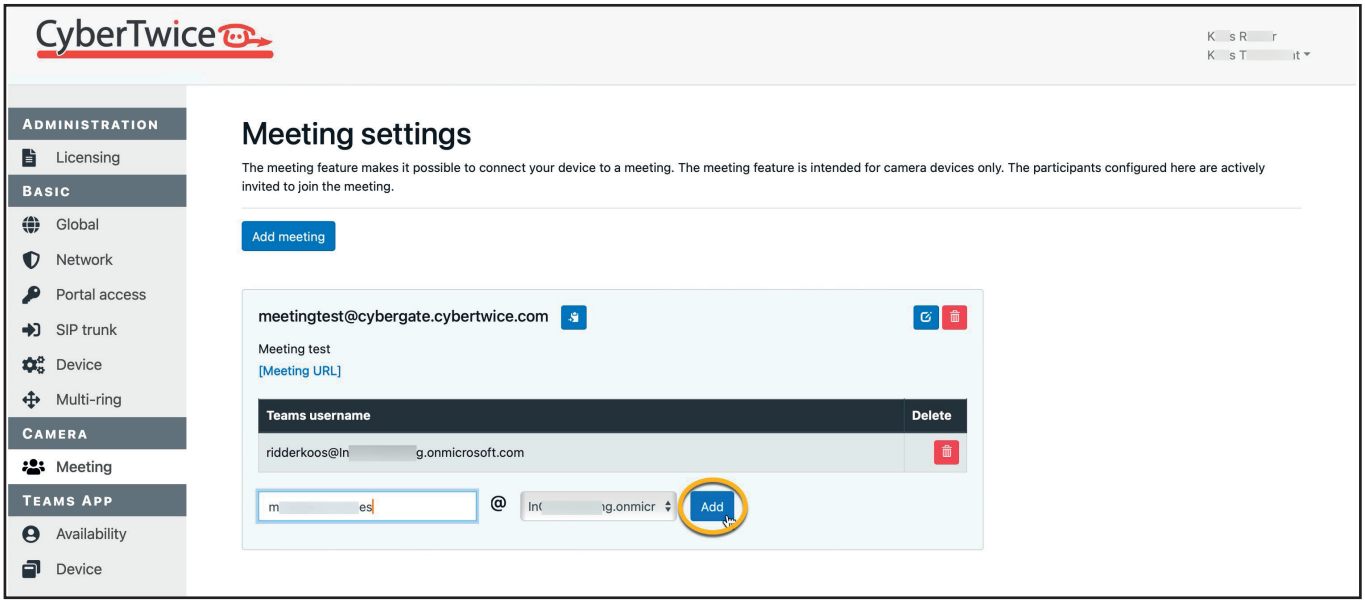

*CyberGate management portal 'Meeting' - 'Add meeting'*

- 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.




*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.

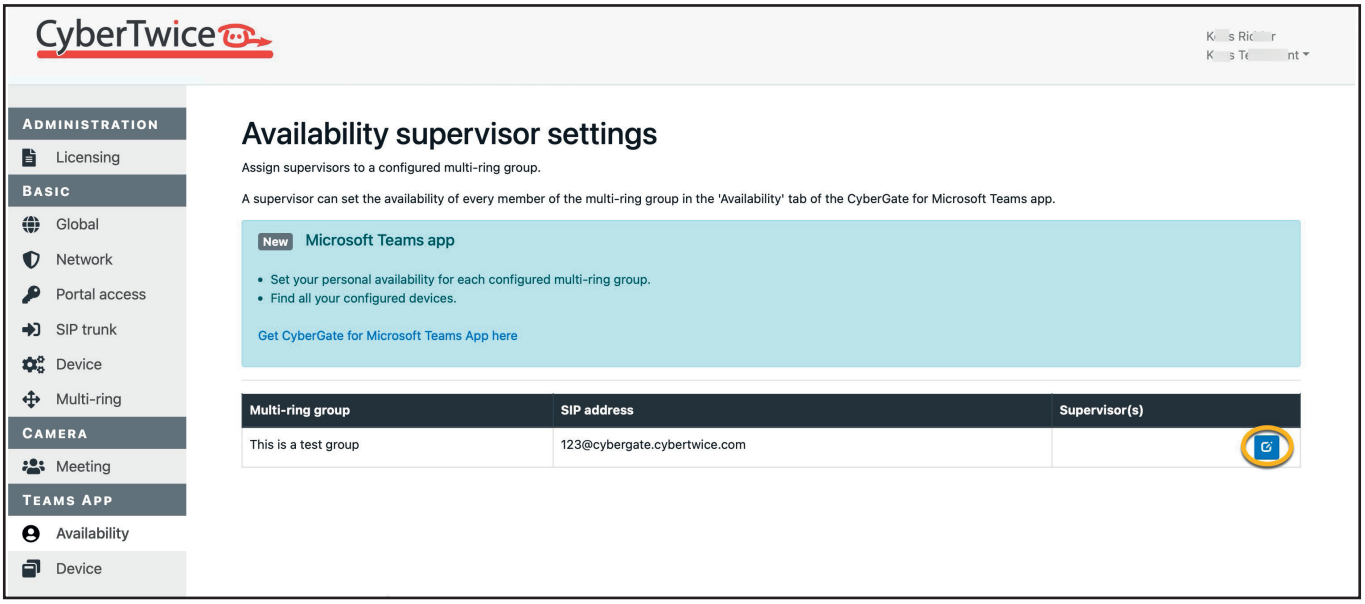
*A Supervisor of a Multi-ring group can perform the following tasks in the CyberGate for Microsoft Teams app:*
- *Can add and delete users in this Multi-ring group*
- *Set the availability for all users in the Multi-ring group*

## Availability

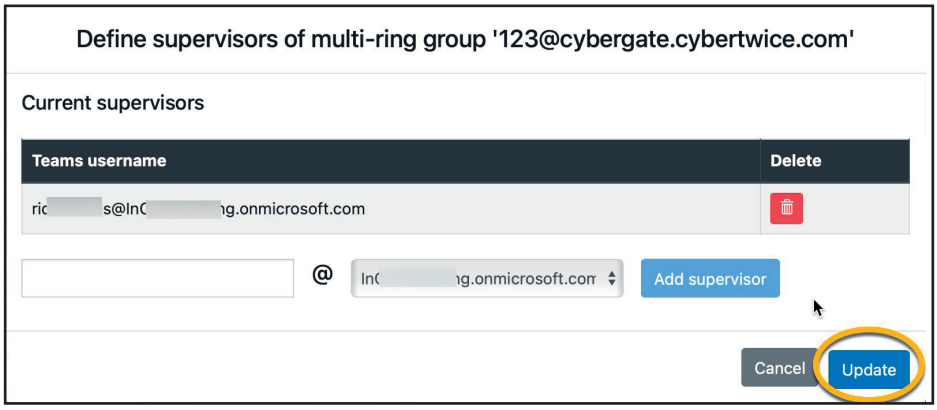
The *Availability* section shows all created Multi-ring groups. By default a Multi-ring group does not have a Supervisor defined as this is an optional feature and not necessary for the functioning of a Multi-ring group.

Add a supervisor:

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

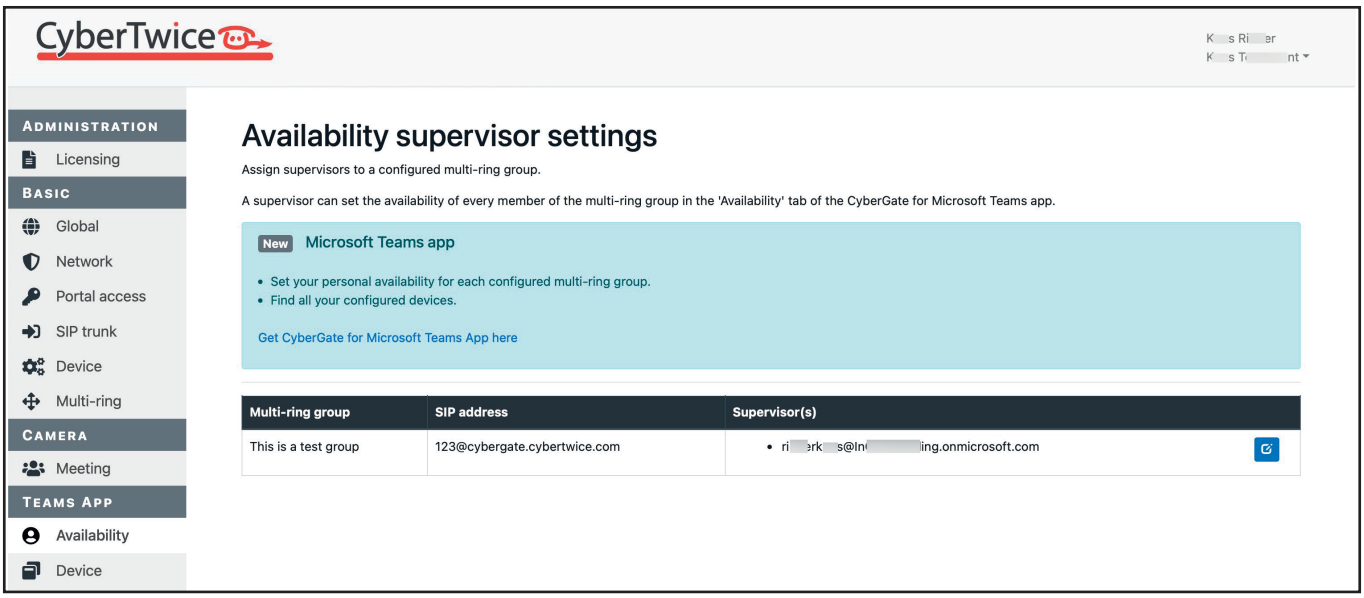



*CyberGate management portal 'Availability' - No Supervisor configured yet*




*CyberGate management portal 'Availability' - Select Supervisor*

- Click 'Update' to save.



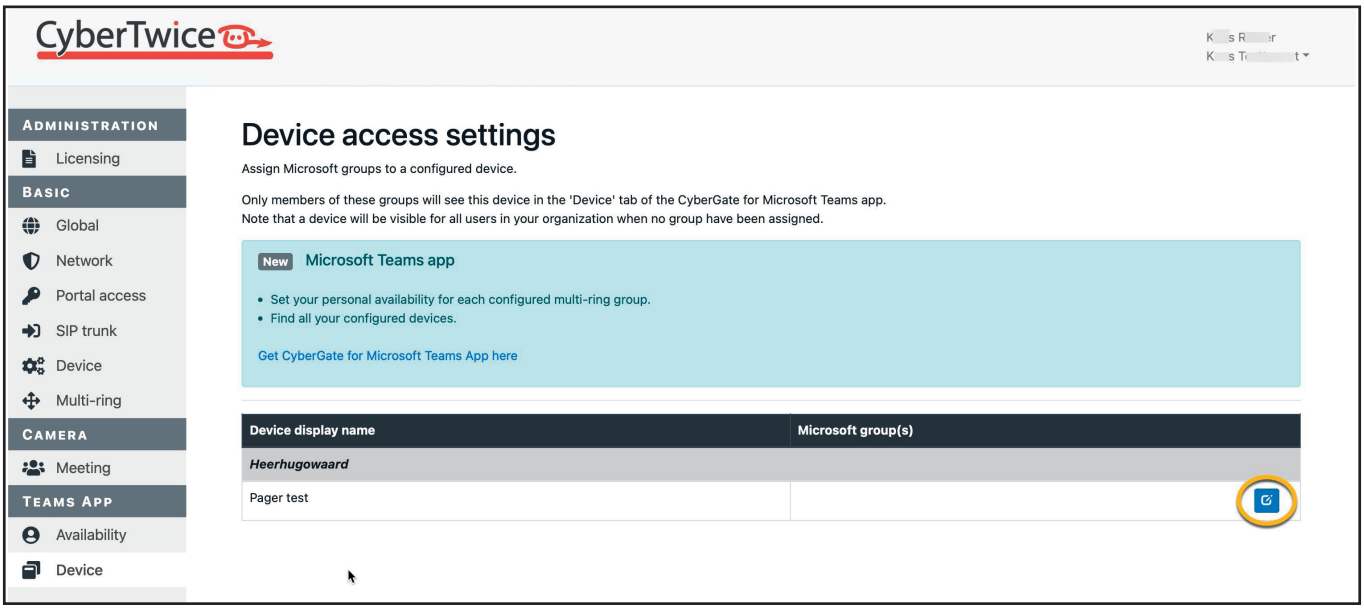

*CyberGate management portal 'Availability' - Supervisor configured*

## 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).

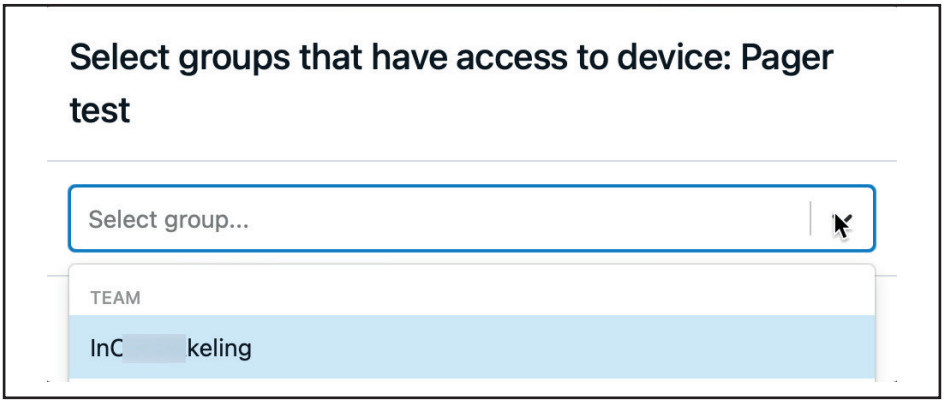
Add a group:

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



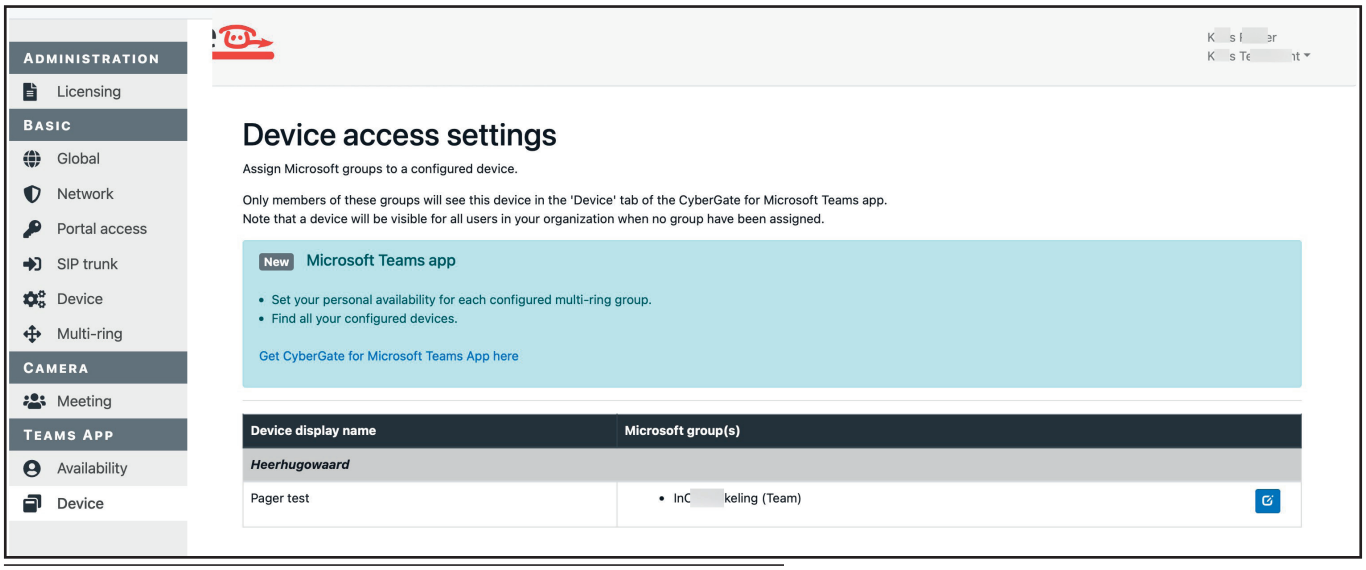

*CyberGate management portal 'Device' - No Group configured yet*

- 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*

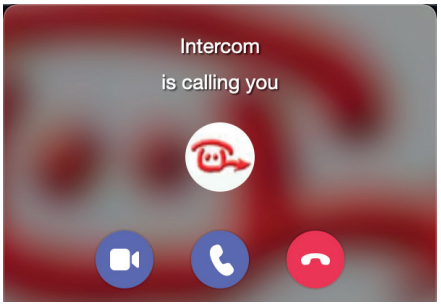
- Click 'Update' to save.




*CyberGate management portal 'Device' - Group configured*

# Appendix B: Configure the display name of the device

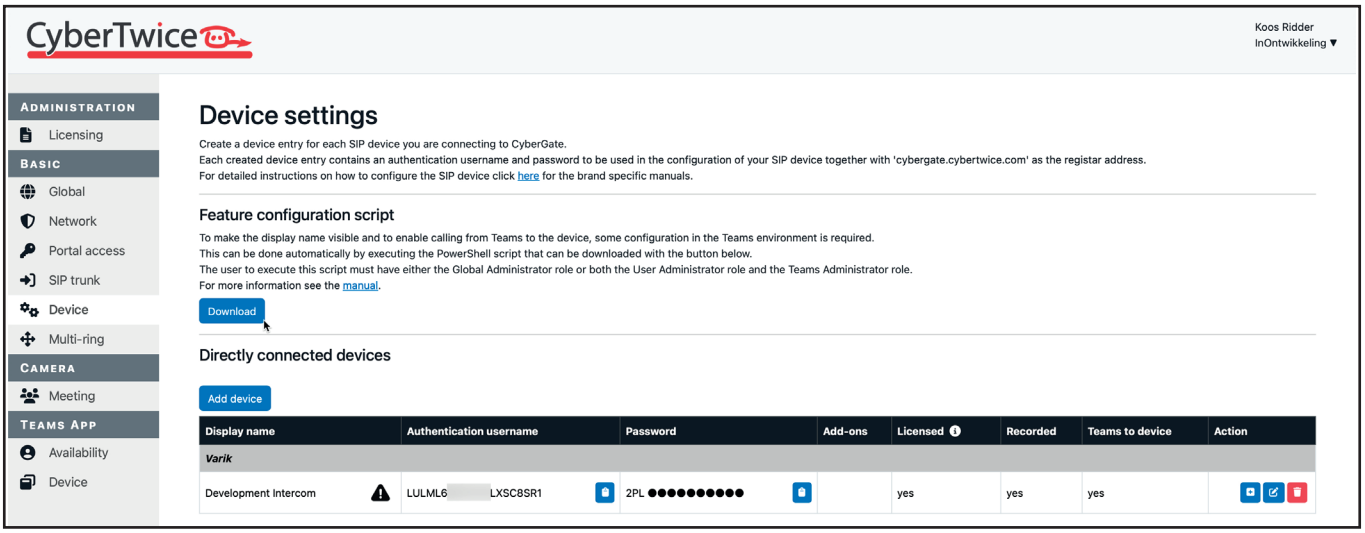
By default, incoming calls from the device will be announced in Teams as 'Intercom'.




*Microsoft Teams incoming call with the default name 'Intercom'*

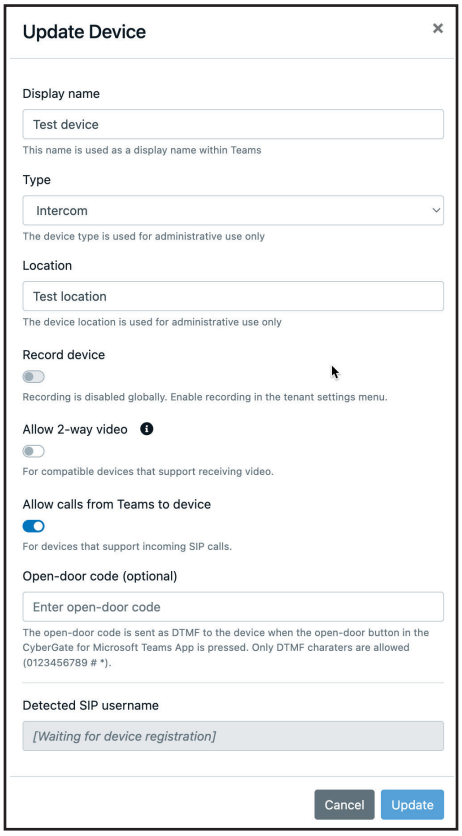
If you have multiple devices configured in CyberGate or you would like to show another name in Teams you can modify the name per configured device.

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

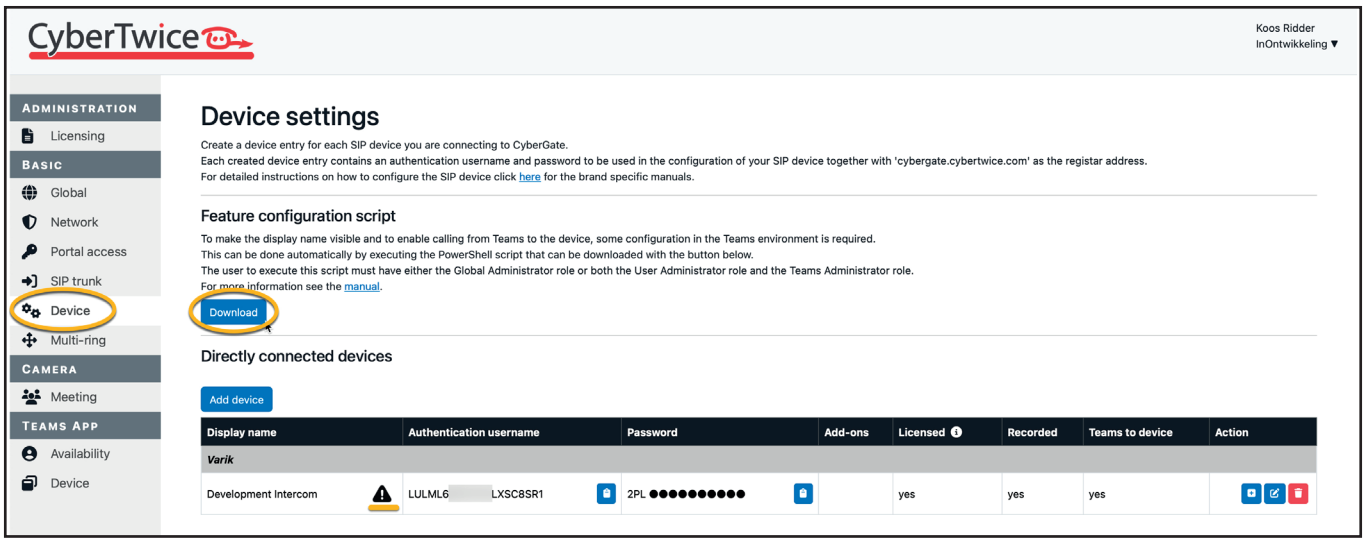



*CyberGate management portal 'Device' - Default 'Display name'*

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'.



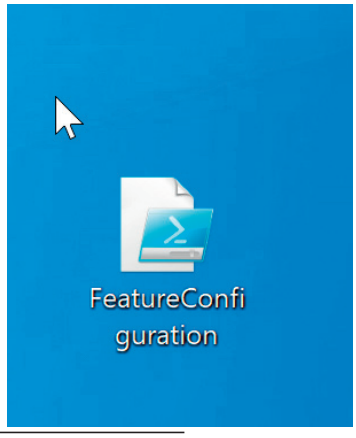

*CyberGate management portal 'Device settings' - 'Update device'*




*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.

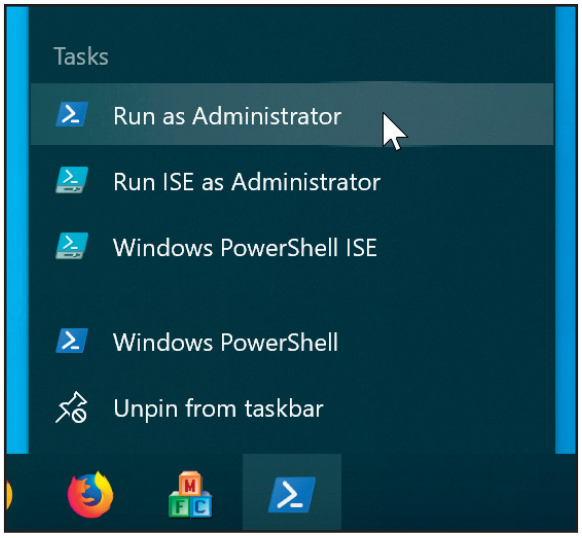
1. Make sure you have a PC with Microsoft PowerShell installed.
2. Click on the blue 'Download' button to download the script




*Microsoft Windows - Downloaded PowerShell script*

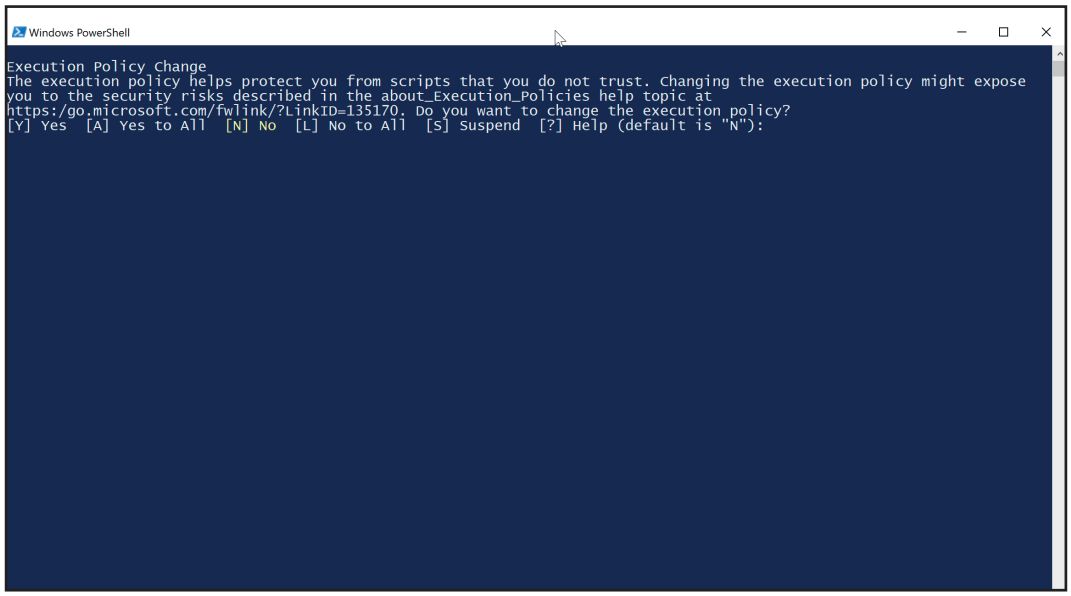
3. Right-click on Powershell and select 'Run as Administrator.

*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!*



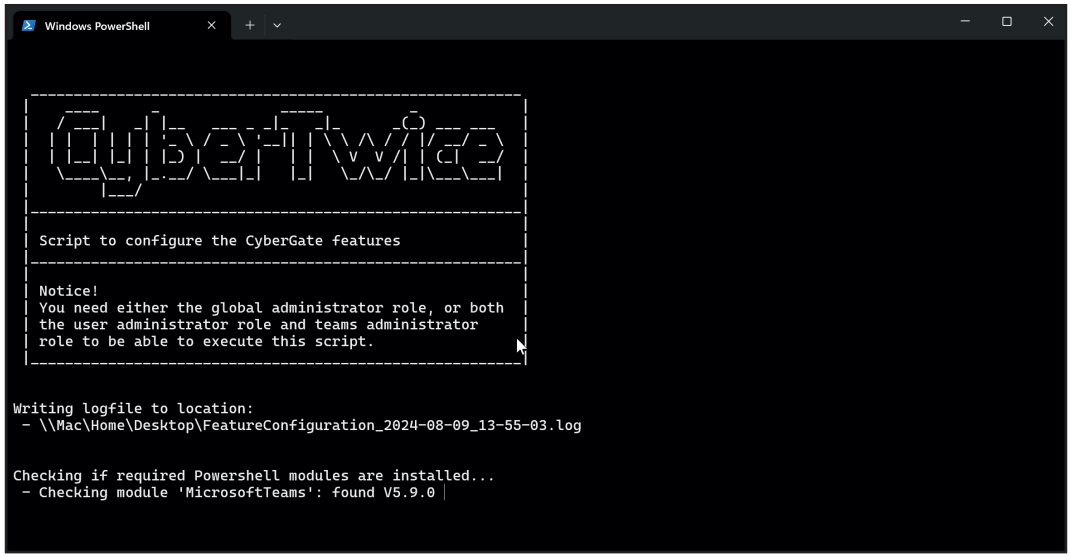

*Microsoft Windows - 'Run as Administrator'*

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



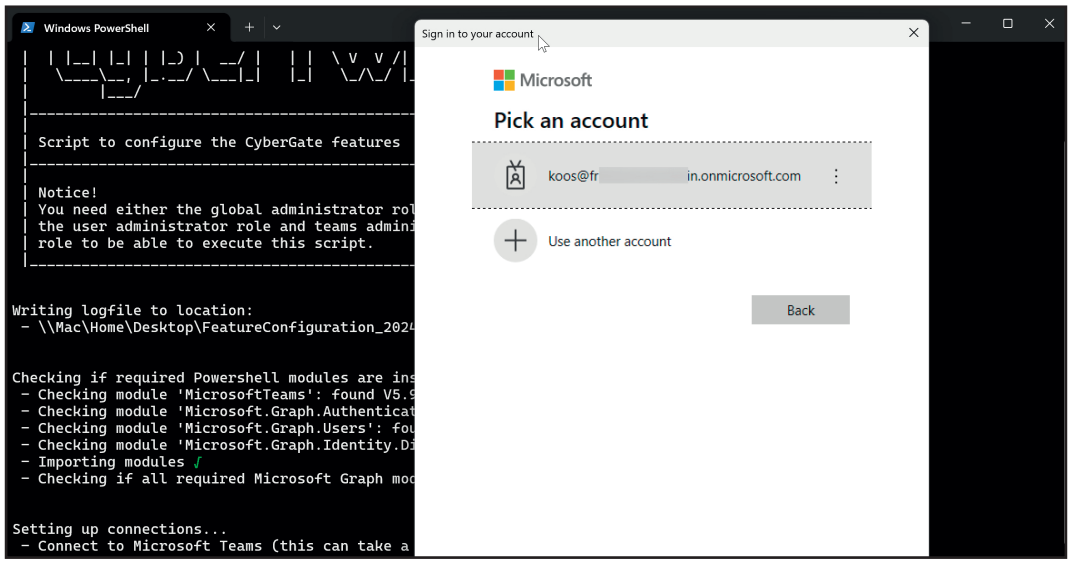

*Microsoft PowerShell - 'Execution Policy Change'*

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




*Microsoft PowerShell - 'Azure user name'*

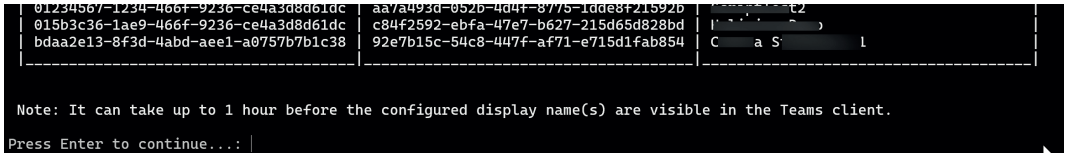
6. Enter your password to login at Microsoft.




*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.




*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**

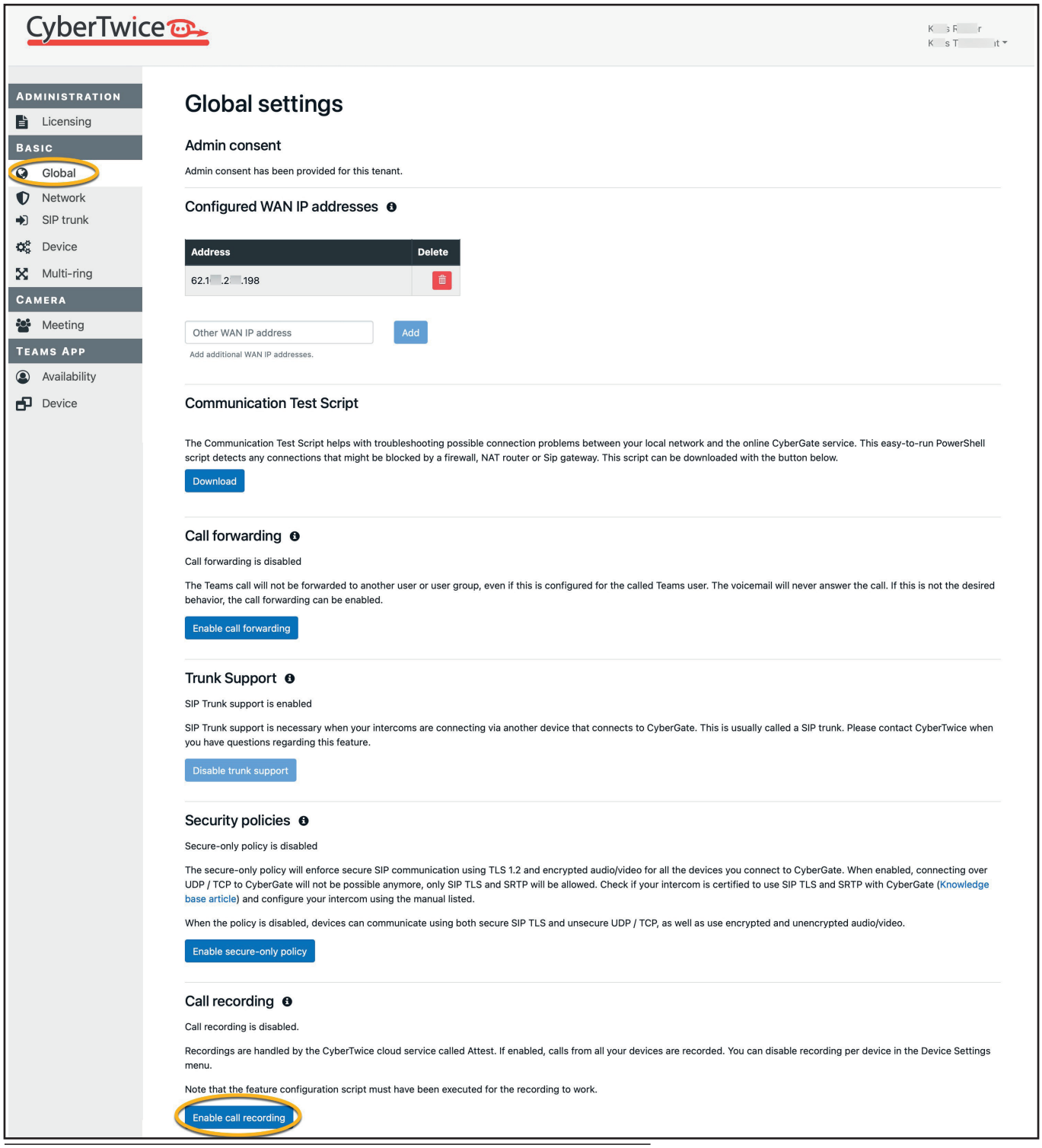
**“Modify the recording related settings” on page 59**

**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*).

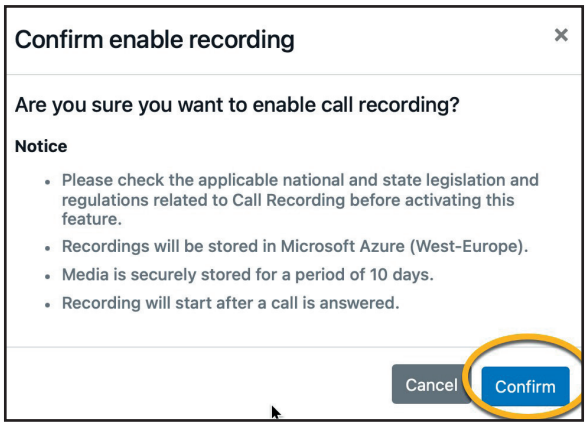
- The first step is to login to the Cybergate Management portal using your Microsoft credentials and navigate to Basic-Global. Scroll down to the 'Call recording' section.




*CyberGate management portal 'Global' - Call recording disabled*

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

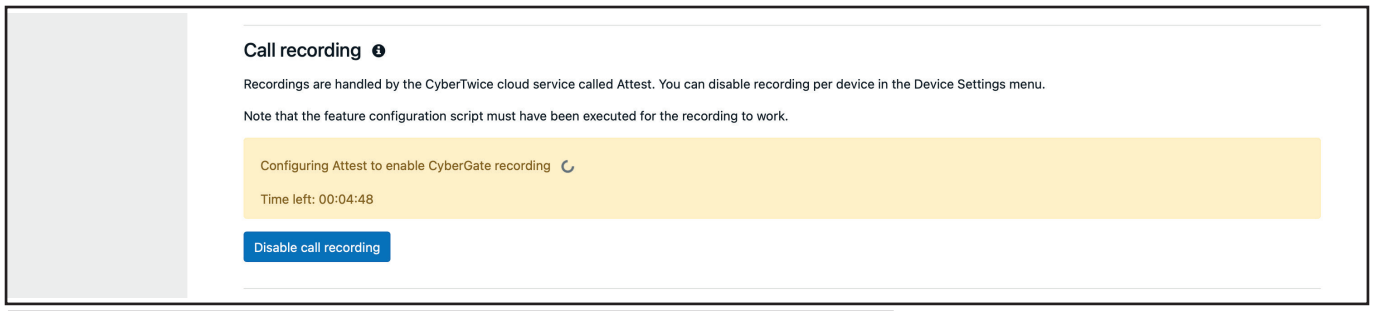
*Note:*
*Call recording can only be enabled if the Feature Configuration PowerShell script has been run at least once. See Appendix B: Configure the display name of the device for instructions on how to run this script.*




*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.



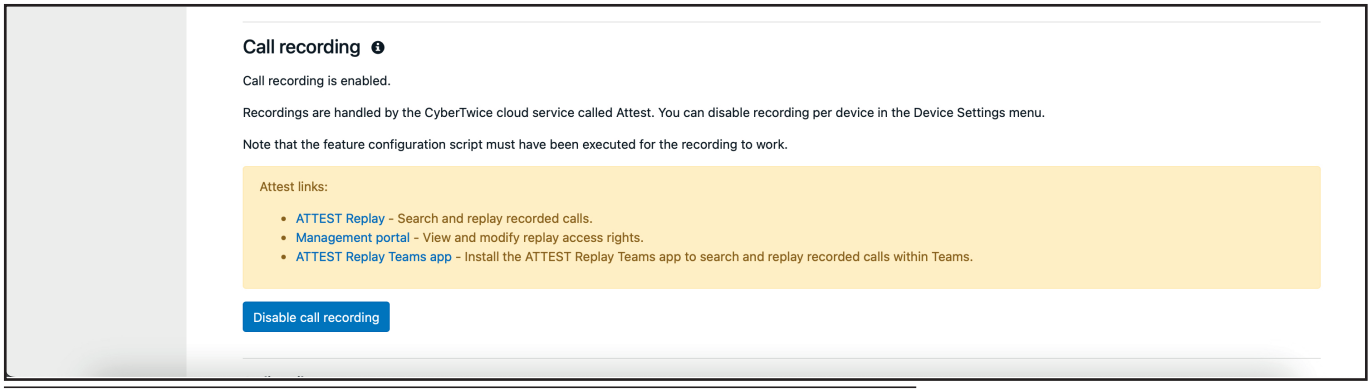

*CyberGate management portal 'Global' - Call recording configuring*

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.*

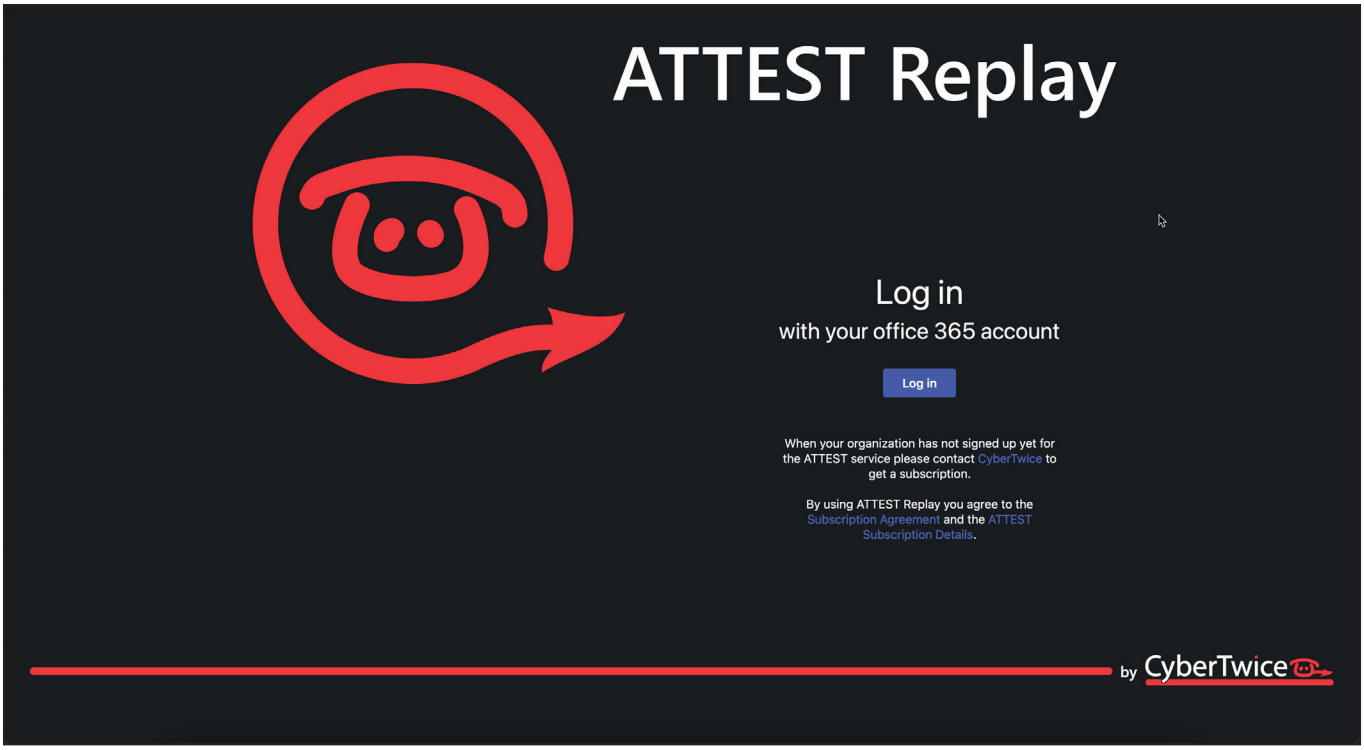
## Search and replay recorded calls

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

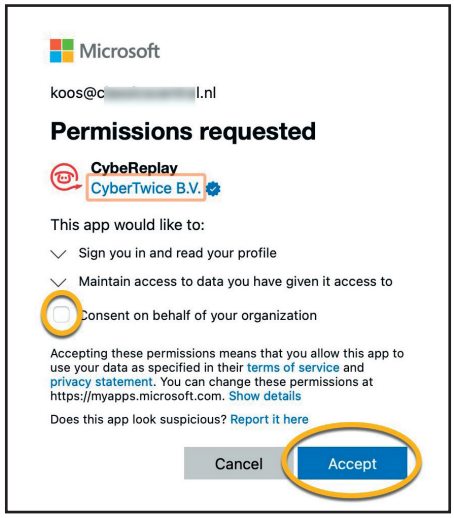
You can access ATTEST Replay using your Microsoft credentials.




*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

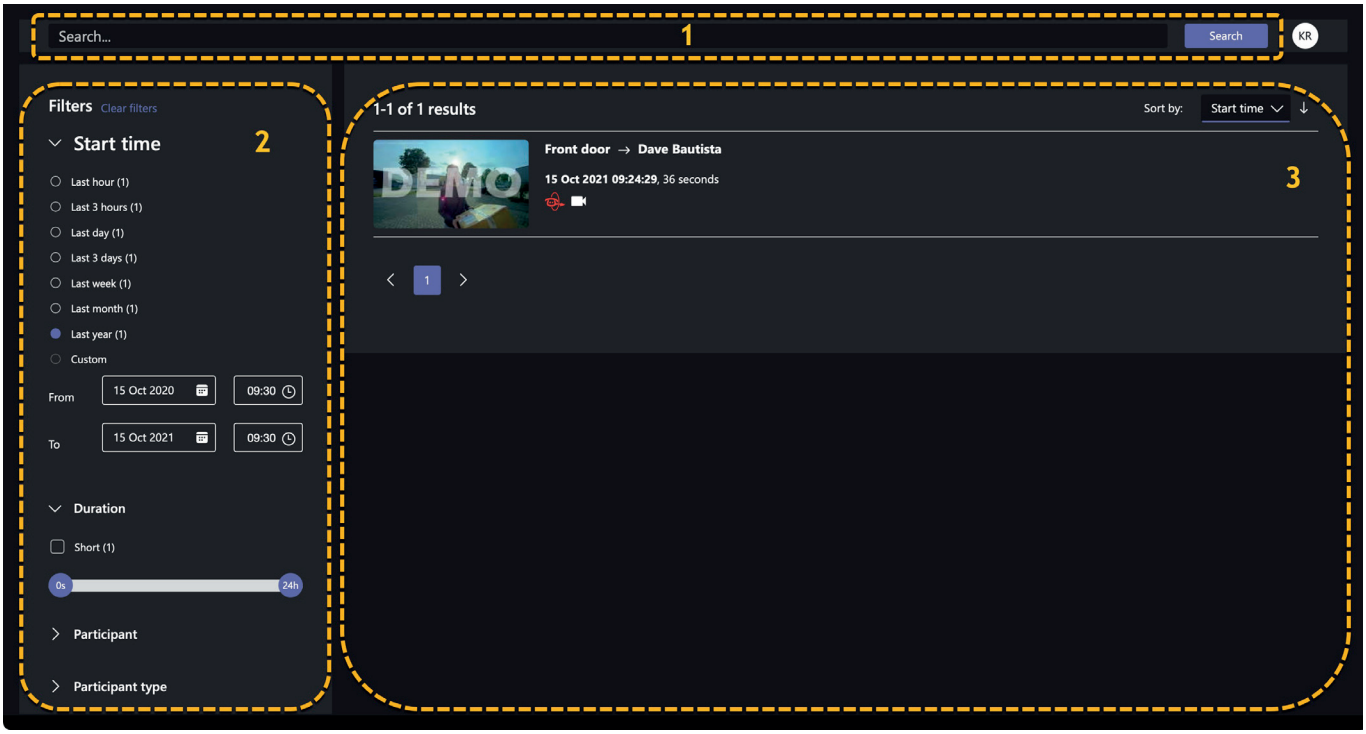



*Microsofts 'Permissions requested' window - for ATTEST Replay*

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

The Search screen is devided 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.

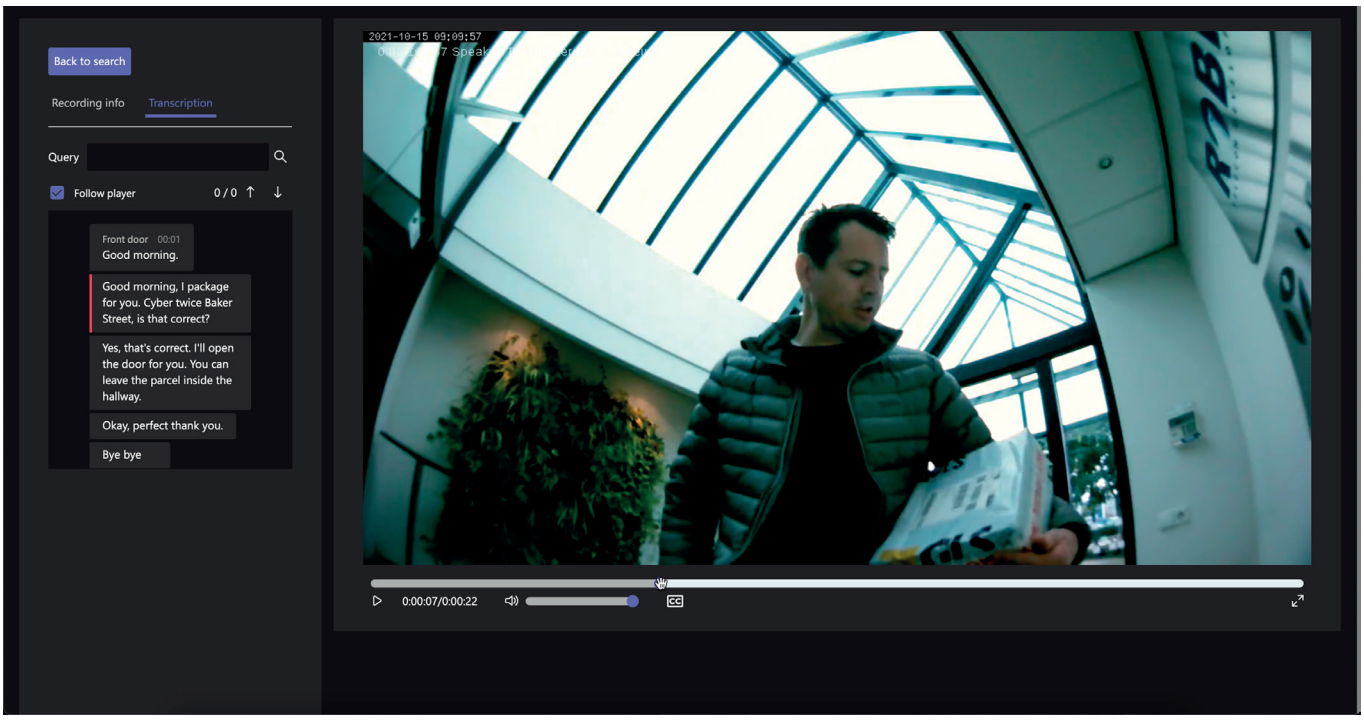
A card consists of:

- 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:

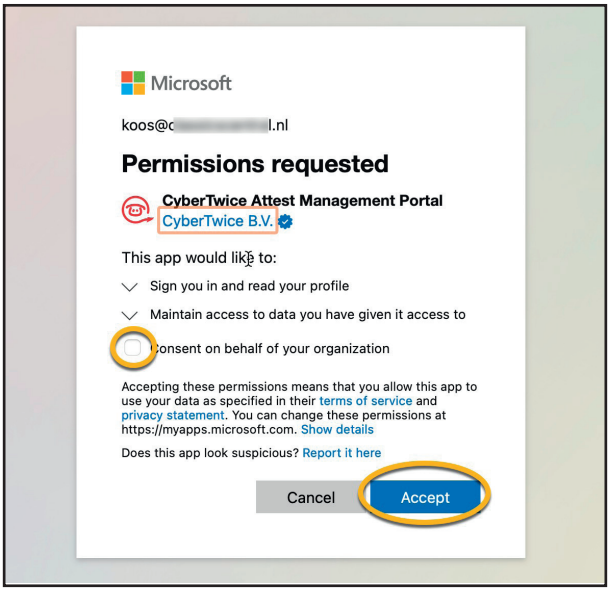
- See the Recording info
- See the Transcription of the recording with the option to follow the player (when available)
- Play the recording
- Pause the recording
- Skip through the recording
- Control the playback volume
- Enable / disable subtitling
- Change to full screen
- Return to the search results

## 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*. *(URL: https://admin.attest.cybertwice.com)*

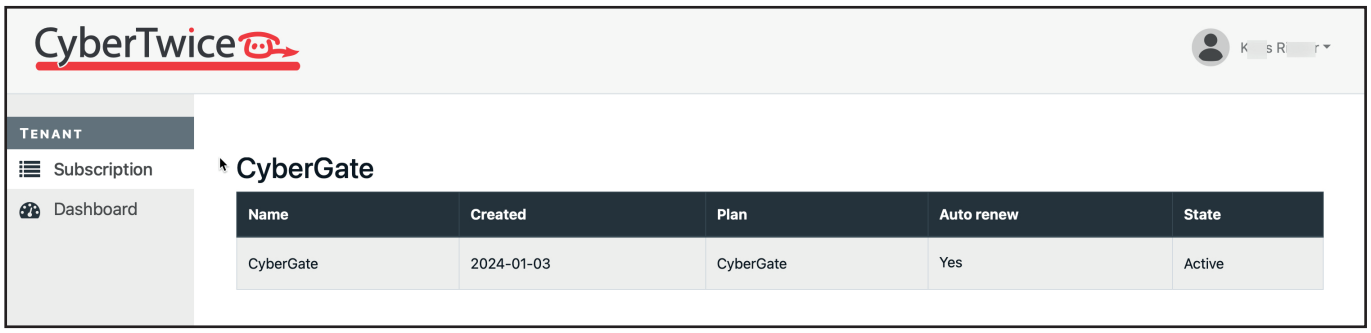
- Log into the ATTEST Management portal as an *Administrator*.

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.



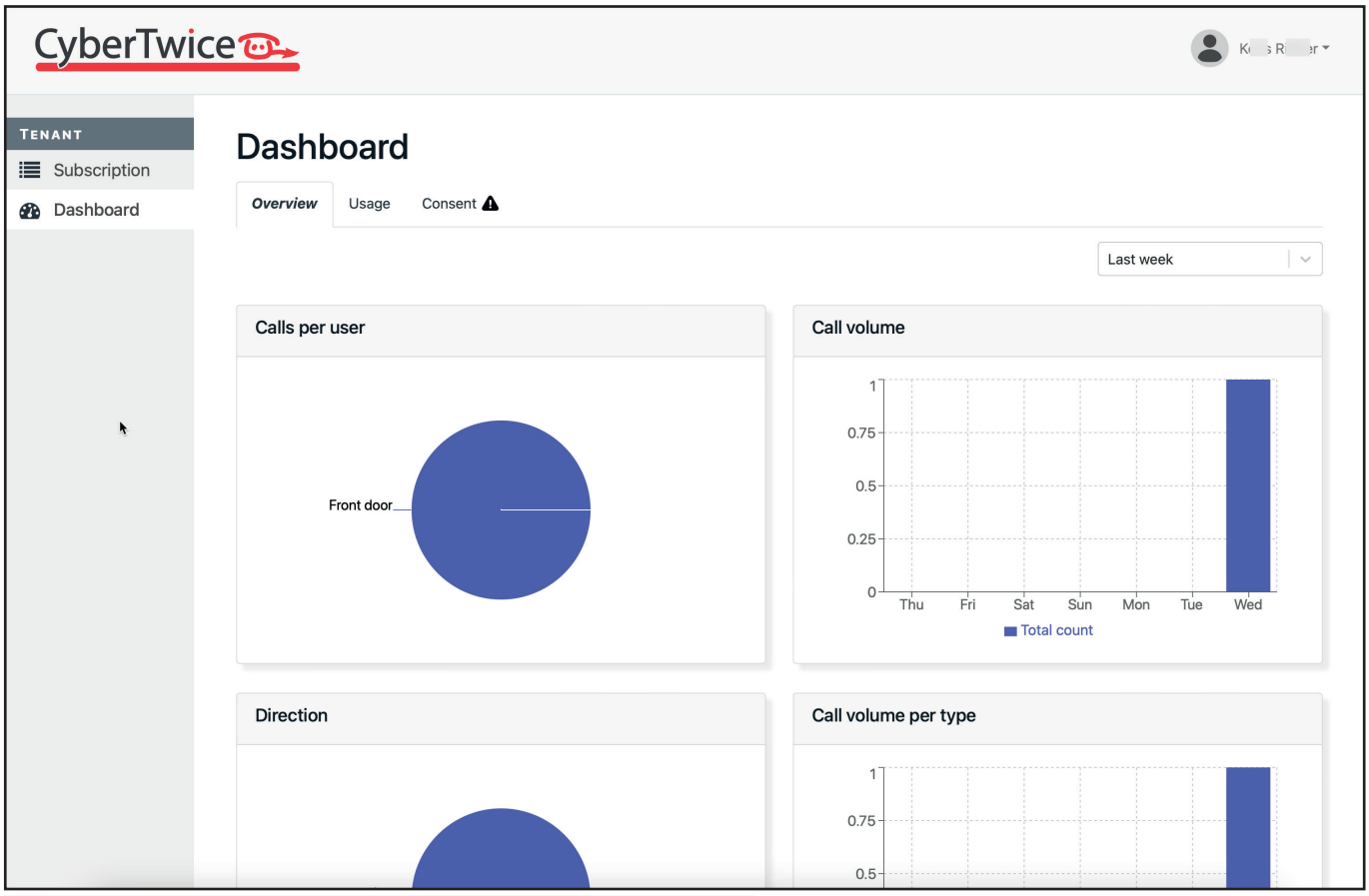

*ATTEST management portal 'Permissions request'*

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




*ATTEST management portal 'Subscription'*

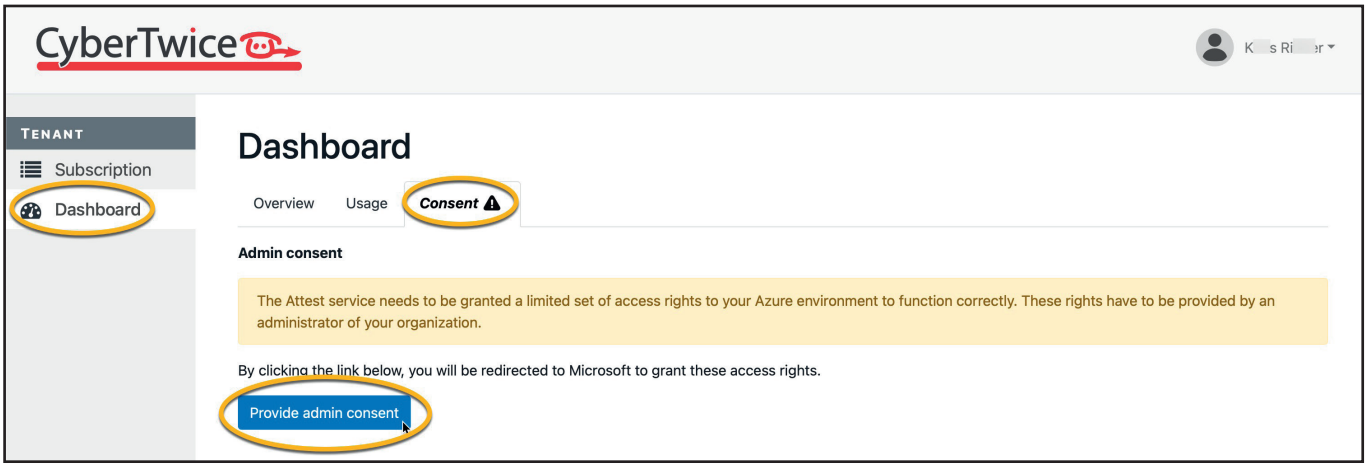
- Click on 'Dashboard' to show a graphical overview related to the recorded calls.




*ATTEST management portal 'Dashboard' - 'Overview' tab*

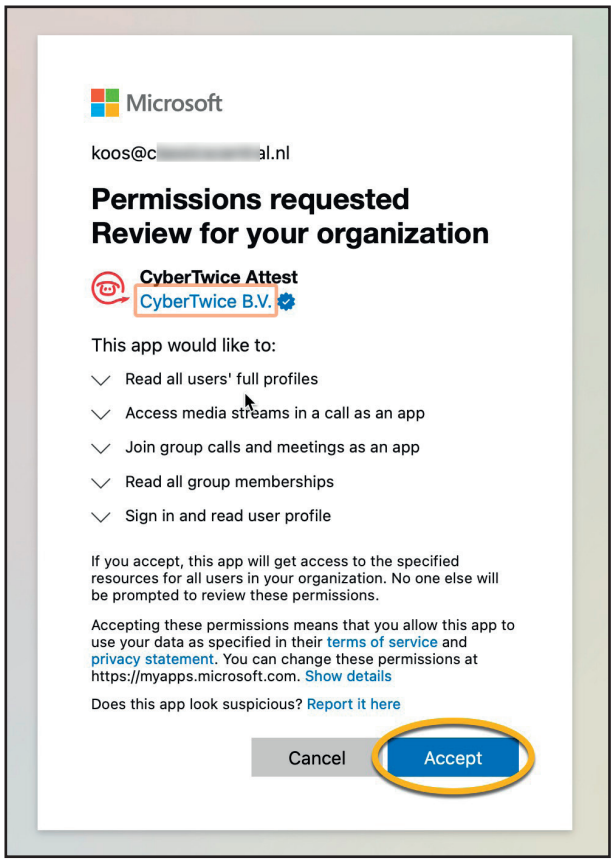
Before any recording related settings can be modified, consent has to be given to ATTEST.

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



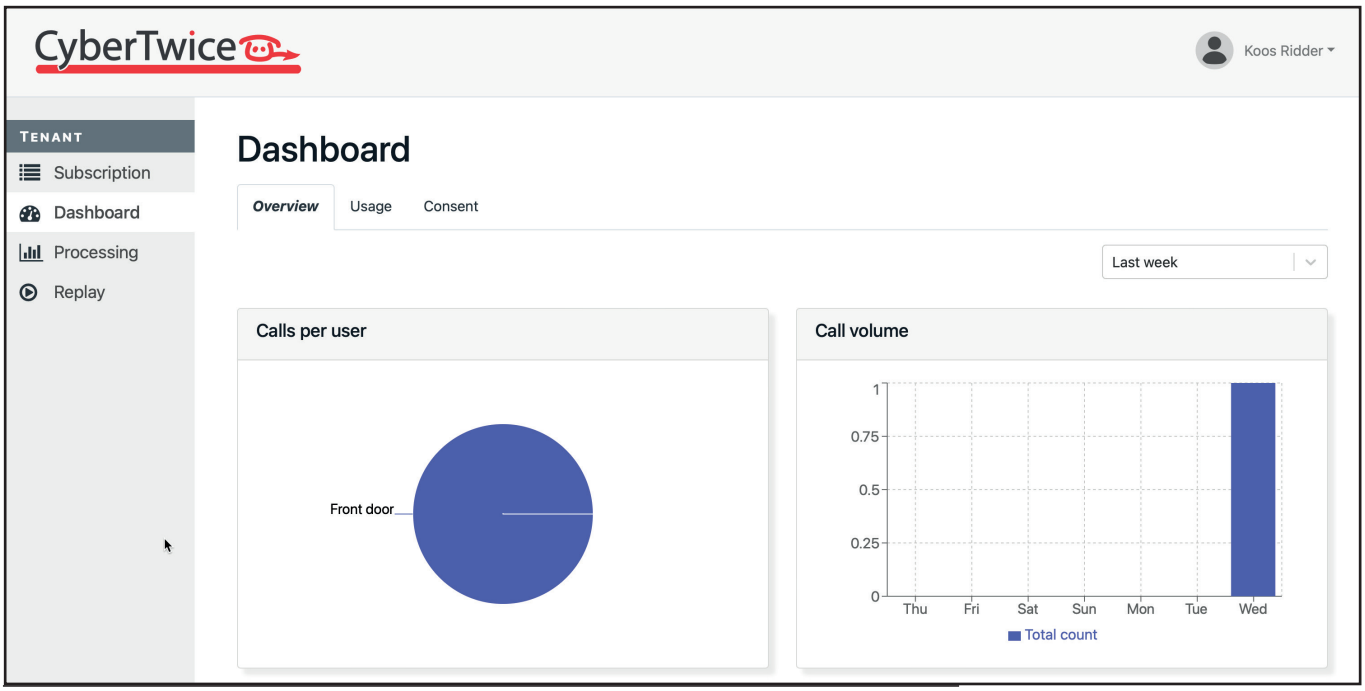

*ATTEST management portal 'Dashboard' - 'Consent' tab*

- 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.

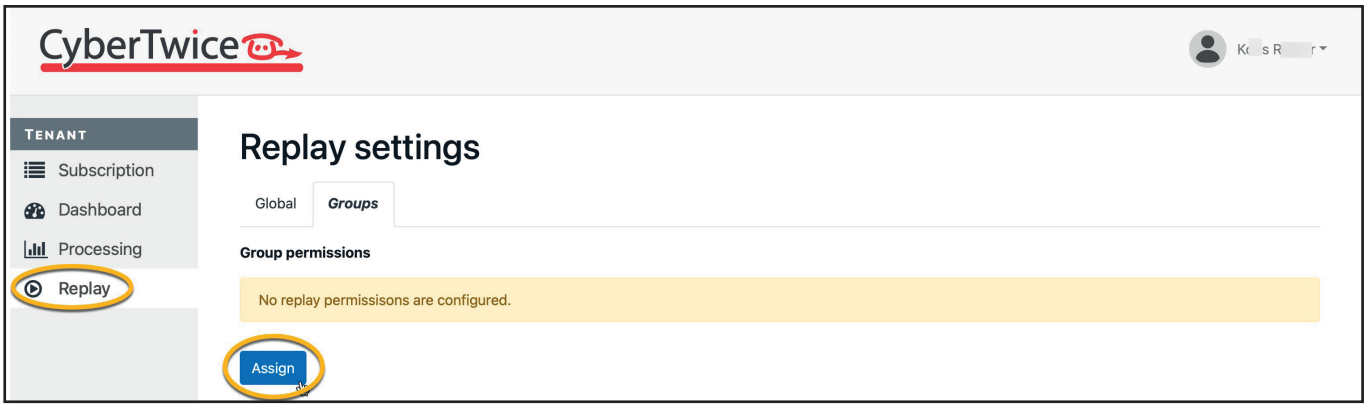



*ATTEST management portal 'Dashboard' - 'Overview' tab, consent given*

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!*

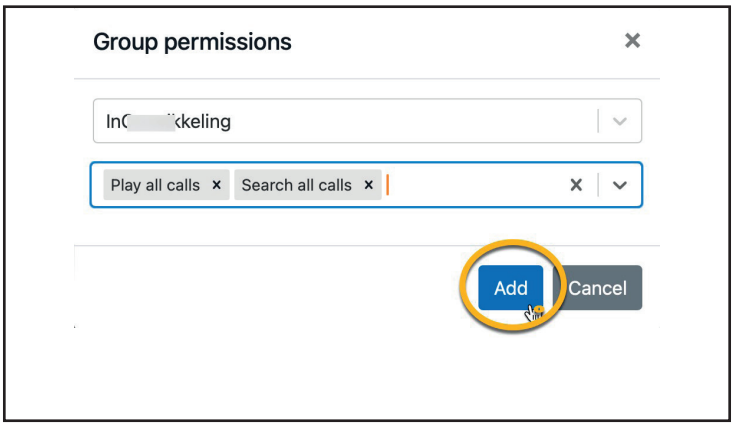
- Click on the 'Groups' tab to set group permissions.



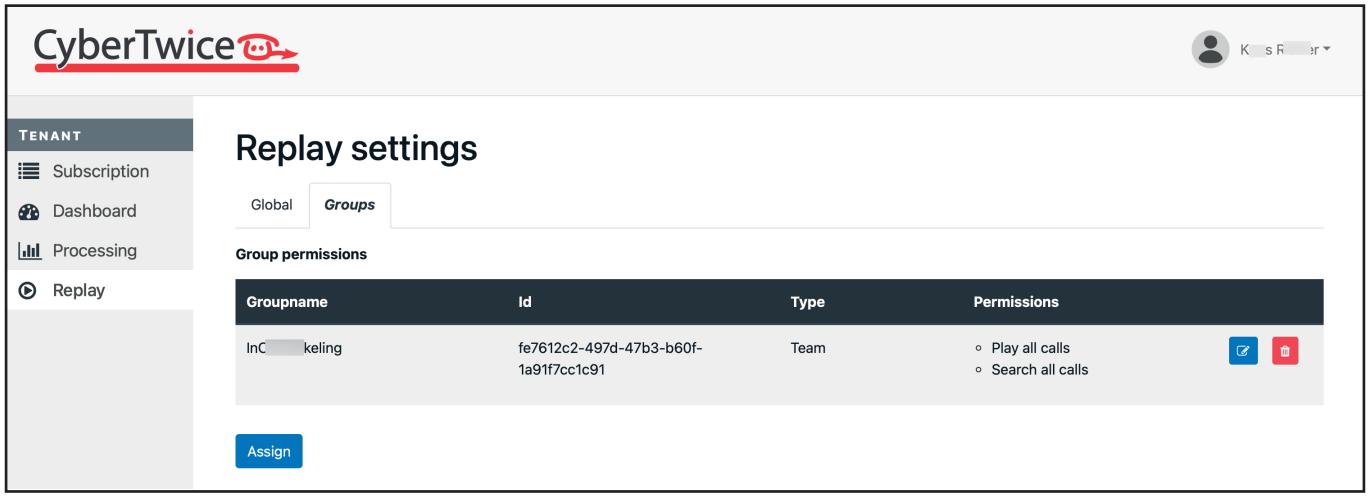

*ATTEST management portal 'Replay' - 'Groups' tab*

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*




*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 visable 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.

## 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 |