Anywhere365®

# Attendant Console for Microsoft Teams

## Compliance information

April 2022

Workstreampeople

MANAGEMENTSYSTEEM CERTIFICATIE DNV·GL NEN 7510

MANAGEMENTSYSTEEM CERTIFICATIE DNV·GL ISO 27001

**WORKSTREAMPEOPLE BV**
Van Nelleweg 1 Hal B
3044 BC Rotterdam

Tel +1 206 338 7450
www.anywhere365.io
info@anywhere365.io

July 2020, Version 1.3.3

Author: Workstreampeople

This document contains confidential and proprietary information which may be legally privileged. It is intended only for the original recipient. Any form of reproduction, dissemination, copying, disclosure, modification, distribution and or publication of this material is strictly prohibited without the explicit consent of WORKSTREAMPEOPLE. All products mentioned in this and associated documents are the property of their respective owners. All rights reserved © 2020 WORKSTREAMPEOPLE

# Table of Contents


.....1
Table of Contents .....3
Anywhere365 SaaS Platform Architecture .....4
Overview .....4
Authentication .....4
Provisioning .....4
Tenant segregation .....4
Customer data maintained by Anywhere365 .....5
Tenant level settings .....5
User data .....5
Technical data .....5
Admin approval .....6
Admin approval for the Teams Bot .....9
Data retention policy .....10
Personal user data .....10
Tenant settings .....10
Logging data .....10
Data residency .....11
Security validation .....12
More resources .....14

## Anywhere365 for Microsoft Teams

This document describes compliance-related aspects of the Anywhere365 SaaS platform.

- *Note: This is not a legal document; it aims to provide an overview of the architecture and compliance-related policies.*

# Anywhere365 SaaS Platform Architecture

### Overview

The Anywhere365 SaaS platform is a modern, multi-tenant platform developed for SaaS solutions

The platform is hosted in Microsoft Azure.

### Authentication

For authentication, the standard Microsoft Authentication mechanism is used. As the authentication is handled by and hosted by Microsoft, Anywhere365 does not have access to the user credentials.

When using the Team app, we rely on Microsoft SSO for Teams Apps.

### Provisioning

The Anywhere365 SaaS platform was designed for auto-provisioning. When a user logs in for the first time, a customer tenant and user profile are created automatically.

### Tenant segregation

Customer data is stored in a dedicated customer tenant. Each tenant has a unique set of credentials that only allows access to the data within the customer tenant.

# Customer data maintained by Anywhere365

### Tenant level settings

Some configuration is stored at tenant (customer) level. This includes queue configuration and calendar and mail settings.

### User data

The following data is stored by Anywhere365 inside the customer tenant:

- Personal contacts
- Contact notes
- Favorites
- Preferences such as layout, user-interface language and queue subscriptions

### Technical data

The platform also stores data needed for the proper functioning of the solution.

#### *Cache data*

Cache data is temporary data, used to optimize the performance and responsiveness of the solution.

All cache data is time-limited; it will be discarded or refreshed after a certain amount of time.

Data can be cached on the client or the server. Personal data cached on the client is always encrypted to prevent unauthorized access.

#### *Logging data*

Standard logging does not include personally identifiable information.

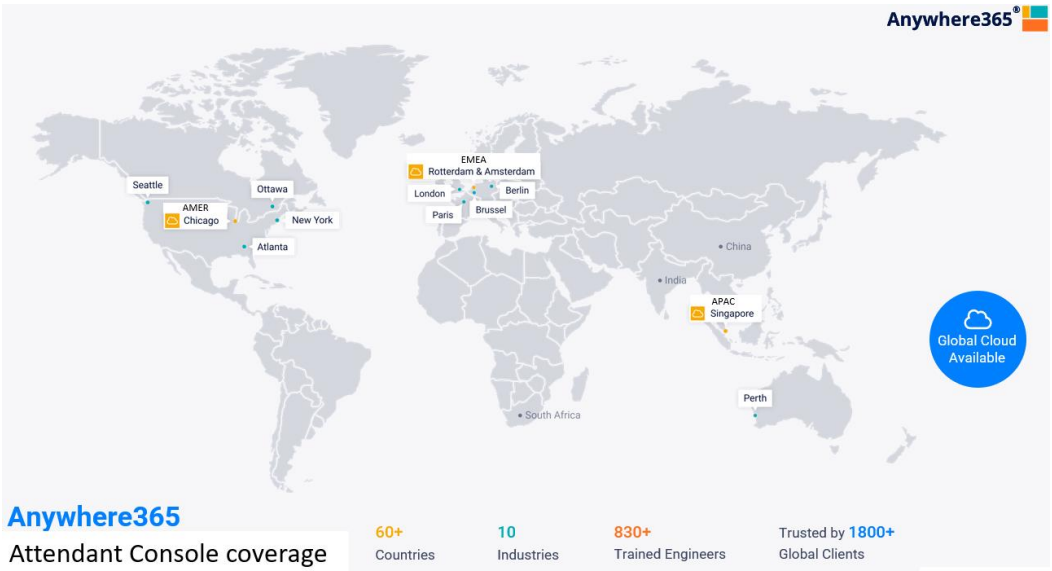
However, when investigating customer issues, Anywhere365 might need to temporarily elevate the log level to obtain detailed data required to analyze the behavior.  In case this log data contains personally identifiable information, it will only be handled by persons who are authorized to do so.

As soon as the inspection is completed, to log level will be returned to normal.

# Azure Region

Anywhere365 Attendant service is available from 3 main Azure Regions. Besides EMEA, the Attendant Console has now a regional presence in the Americas and Asia-Pacific region.

- EMEA Europe Azure Region: Amsterdam
- AMER American Azure Region: Iowa
- APAC Asia-Pacific Azure Region: Singapore



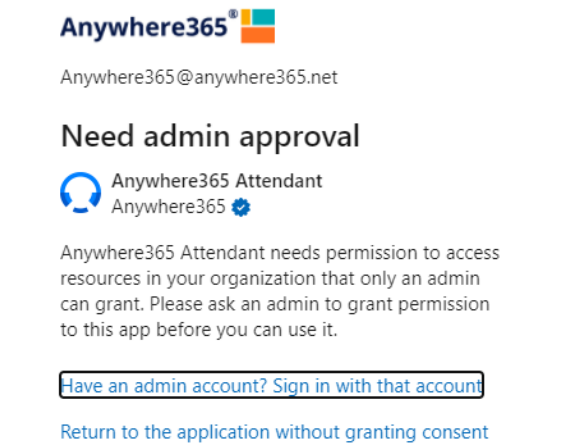
# Admin approval

For the Attendant Console to function correctly, it needs access to specific Office 365 resources of the customer's organization.

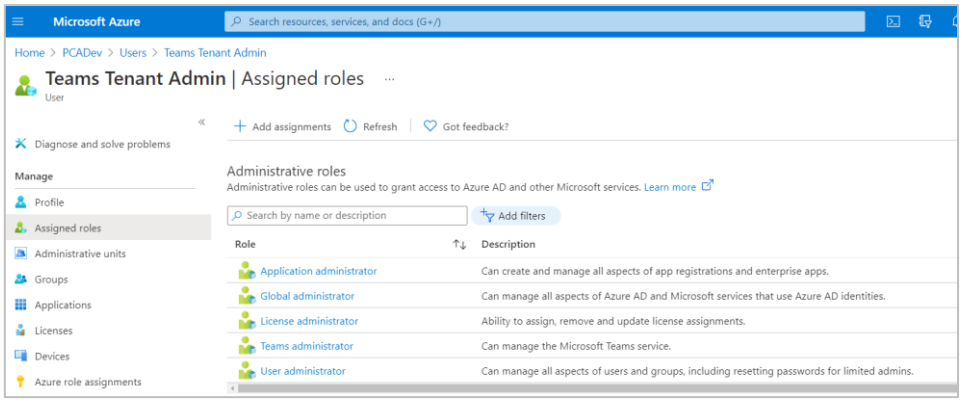
An administrator must grant access to these resources. As long as an administrator has not granted access, users will see a popup like this one.

This popup will appear once time, if you ask a trial license for an Attendant Console user that has no admin roles, and on a tenant that has not been consent.

Once consent, you will not have it again for instance when ordering new Attendant Console user license.

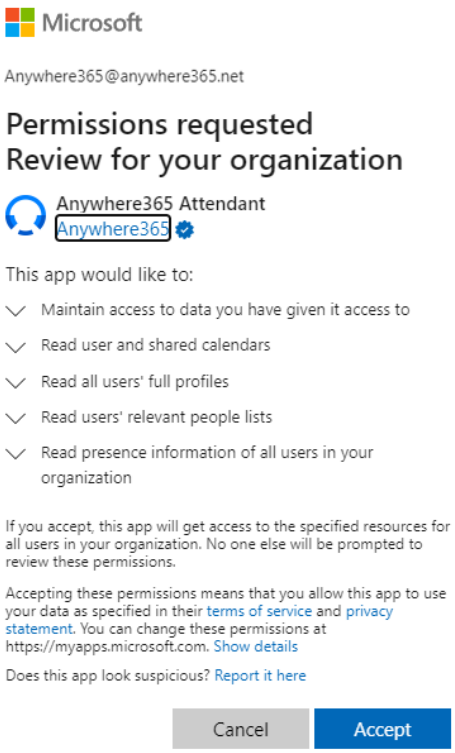



An admin user must have the following roles:



Administrators will be presented with an overview of the request permissions and have the option to grant access (consent).

### Admin Approval for the Front End



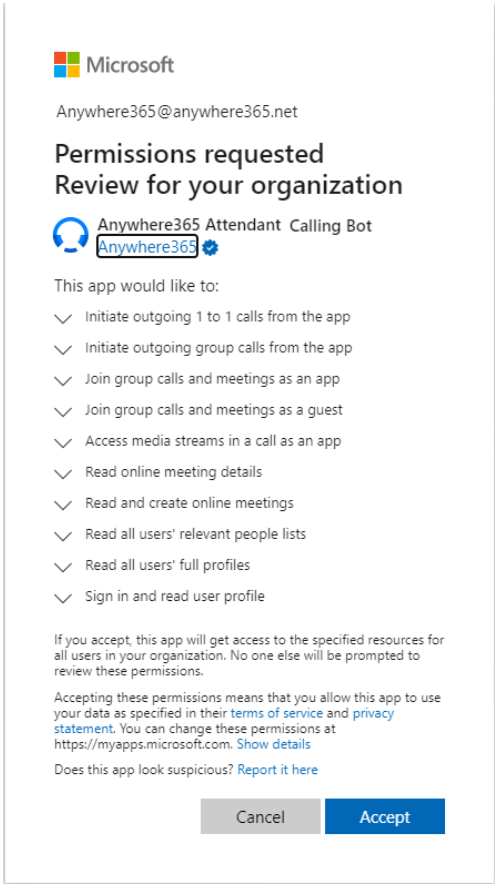

Currently, Anywhere365 requires the following permissions:

- Read all users' full profiles
  - Read contact photo and other contact details
- Read presence information of all users in your organization
  - Read presence status for contacts
- Read user relevant people lists
  - Read contact details such as telephone number
- Sign in and read the user profile
  - Sign in (automatically) an read user details
- Maintain access to data you have given access to
  - Durable access to above-mentioned resources

*Note: the exact list of requested permission might change over time.*

## Admin approval for the Teams Bot per Azure Region

Via the Admin Portal that is delivered with the Attendant Console, an administrator can give admin consent for the Teams Bot App registration.




Currently, the permissions that are needed for the Teams Bot are :

- Access media streams in a call as an app
- Initiate outgoing 1 to 1 calls from the app
- Initiate outgoing group calls from the app
- Join group calls and meetings as an app
- Join group calls and meetings as a guest
- Read directory data
- Read online meeting details
- Read and create online meetings
- Read all users' relevant people lists
- Read all users' full profile
- Sign in and read user profile

*Note: the exact list of requested permission might change over time.*

# Data retention policy

Data retention covers three areas: user data, customer settings, and logging data.

### Personal user data

The personal user data is maintained by the SaaS platform for as long as the user has a valid subscription.

After the subscription is terminated or disabled, the user data will be maintained for 90 days. This allows the users to reenable the subscription within this period.

After these 90 days the user data will be deleted (purged) and can no longer be recovered.

The personal user data can also be deleted upon a formal, verified request from the user. This will include the subscription itself. It can take up to 14 days for this request to be completed.

### Tenant settings

When the last user of a tenant has been deleted, the tenant (customer) and its configuration is deleted automatically.

### Logging data

Logging data is maintained for up to a week, unless it is used during investigation of issues. This data will be deleted after the issue has been closed.

# Data residency

When enrolling a new customer, the primary and backup region are chosen. Customer data will never be stored outside of these regions.

Data for European customers resides in the West Europa region, which is located in Amsterdam. North Europe region (Dublin) is used for backups and fallback.

Customer information are stored in an isolated, secured and encrypted database.

# Security validation

The Anywhere365 SaaS platform was architected using the secure-by-design principle.

Security has been tested and verified by an independent third party.

We also perform internal OWASP compliance test and penetration tests (pentest) at regular interval to ensure the security of our solution.

Anywhere365 SaaS platform is ISO-27001 certified. SOC-2 certification is in progress.

## Anywhere365 Dialogue Cloud

Anywhere365 Dialogue Cloud delivers the reliability and security modern omni-channel contact centers demand while allowing you the flexibility to easily integrate your back-office systems and the latest technologies into your agents' workflows.

## Smart routing

Omnichannel dialogue routing allows routing calls based on CLID, Bots, skills, geography, IVR prompts, CRM data, IOT devices, etc.

## Chat- and Voicebots

Self-learning Azure AI Bots handle routine voice and chat interactions leaving the complex dialogues for live agents.

## IVR - ICR (Integrated Chat Response)

Create menus and route calls/chats based on customer input in a flexible and easy to manage menu. Azure Cognitive Services provide real-time language detection for speech in 11 languages and chat translation in 60 different languages.

## Business Applications

In addition to supporting Microsoft Skype for Business and Teams clients, Anywhere365 turns Dynamics 365, Salesforce and ServiceNow into powerful communications tools for both contact center agents and regular business users alike.

## Integrations

The Anywhere365 platform integrates with Microsoft Flow, PowerApps, Azure Cognitive Services and over 30 other CRM and ERP solutions.

## Reporting and Dialogue Intelligence

Historical reporting and real-time monitoring of contact center KPI's. Microsoft Power BI tools provide deep-dive actionable intelligence.

# More resources

## Golive!

The GoLive! site https://golive.anywhere365.io/
Explains in detail all aspects of installing, customizing, maintaining or using the software.

## Anywhere365 website

https://anywhere365.io/

## Social media

Follow us on

LinkedIN

Twitter

Watch our product demo's on

YouTube

Anywhere365®

Attendant Console for Microsoft Teams
Compliance information

ROTTERDAM - BRUSSELS - LONDON – MANCHESTER

ATLANTA – OTTAWA – SEATTLE

anywhere365.io