Security and data privacy in Epiphan Connect

This document explains what information Epiphan Connect™ obtains from your Microsoft tenant, its users, their meetings, and how Epiphan keeps that information secure.

Table of contents

- Pairing your Microsoft Teams tenant and Epiphan Connect
  - What permissions are required for Epiphan Connect?
  - Who can use Epiphan Connect in my meetings?
  - How can I revoke permissions for Epiphan Connect?
  - Checking if the connection is still valid
- Information stored by Epiphan Connect
  - What information is stored by Epiphan when using Epiphan Connect?
  - Media content in the meetings
  - Participants and their information
- Architecture
  - Diagram
  - User secrets
  - Application credentials
  - Epiphan Connect instances
- Threat Management
  - Vulnerability scanning
- Availability and Reliability
  - Service Monitoring
- Organizational Security
  - Confidentiality Agreement
  - Employee Security Training
- I'm a security researcher, and I found a vulnerability in Epiphan Connect. How do I report it?

Pairing your Microsoft Teams tenant and Epiphan Connect

In order for Epiphan Connect to be used with your Microsoft tenant, the administrator of the tenant must complete an admin consent process, where the administrator gives their consent for the Epiphan Connect application to join meetings in their tenant. This section describes in detail what permissions have to be granted, their scope, and how and when Epiphan Connect uses those permissions.

What permissions are required for Epiphan Connect?

The tenant administrator must consent to the following list of Microsoft Graph permissions:

- **Join group calls and meetings as a guest** (Calls.JoinGroupCallAsGuest.All): This permission is required for the bot to join group meetings in your organization.
  - Microsoft describes this permission as follows: "*Allows the app to anonymously join group calls and scheduled meetings in your organization, without a signed-in user. The app will be joined as a guest to meetings in your organization."* Please note that the bot will not go through the meeting lobby like a normal guest, and it will also not use an anonymous identity to join your meeting either. Instead, the bot will join as an application to your meeting without going through the lobby.

- **Join group calls and meetings as an app** (*Calls.JoinGroupCall.All*): This permission is also required for the bot to join group meetings in your organization.

- Microsoft describes this permission as follows*: "Allows the app to join group calls and scheduled meetings in your organization, without a signed-in user. The app will be joined with the privileges of a directory user to meetings in your organization".*

- **Access media streams in a call as an app** (Calls.AccessMedia.All): While joined to a meeting, this permission allows the bot to receive the audio and video of the participants that are sharing their camera, microphone, and/or screen in the call.
  - Microsoft describes this permission as follows: "*Allows the app to get direct access to media streams in a call, without a signed-in user.*"

- **Read names and members of all chat threads** (Chat.ReadBasic.All): The application only uses this permission to obtain the name or title of the meeting. When a meeting is created and is not associated with a dedicated Microsoft Teams channel, Microsoft creates a chat thread for the meeting. This chat thread has the same title as the name of the meeting. This allows Epiphan Connect to obtain the name of the meeting without requesting access to sensitive resources like the organizer's calendar. It's important to note that this permission does NOT grant access to any message or shared content in the chat. Although the permission does grant access to the list of people involved in the chat, Epiphan Connect is not requesting this information.
  - Microsoft describes this permission as follows: "*Read names and members of all one-to-one and group chats in Microsoft Teams, without a signed-in user.*".

- **Sign in and read user profile** (User.Read): This is a basic permission for most applications in Microsoft's ecosystem. It allows an application to obtain the basic information of the user that is signed-in. The only time when Epiphan Connect uses this permission is during the initial pairing process between Epiphan Cloud and the Microsoft tenant, and it does so to validate that the user is the administrator of the tenant they are connecting to. The information of that user (including the access token generated during this process) is not saved in our systems.
  - Microsoft describes this permission as follows: "*Allows users to sign in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.*"

Who can use Epiphan Connect in my meetings?

When you pair your Microsoft tenant to Epiphan Connect, you do so on a per-team basis. Epiphan keeps track of which Epiphan Cloud team was used to establish the connection between the Microsoft tenant and Epiphan Connect. Only members of that team are allowed to use Epiphan Connect in meetings organized in your Microsoft tenant.

You might allow multiple Epiphan Cloud teams to use Epiphan Connect in your Microsoft tenant, but to do so, your tenant administrator needs to repeat the application consent process for each individual team.

How can I revoke permissions for Epiphan Connect?

To remove the pairing between a specific Epiphan Cloud team and your Microsoft tenant, sign in to https://go.epiphan.cloud/, select the team you want to unpair, and navigate to ***Settings > Epiphan Connect.*** There you will find controls to unpair your Microsoft tenant from this team.

You can also revoke the permissions granted to the Epiphan Connect application in your Microsoft tenant by going to https://aad.portal.azure.com/ and browsing to ***Enterprise Applications > Epiphan Connect > Properties > Delete***. Note that no Epiphan Cloud team will be able to use Epiphan Connect in your meetings after these permissions are revoked.

If you want to remove the pairing between your tenant and only one specific team in Epiphan Cloud, but you no longer have access to that team, please contact support.

Checking if the connection is still valid

Occasionally, Epiphan Connect will try to check if the pairing between Epiphan Connect and your Microsoft tenant is still valid or if it has issues (e.g., the permissions were revoked in the Azure AD portal). Epiphan Connect does this by trying to obtain an access token in Azure AD using your Microsoft tenant as the audience of the token. If the access token is successfully returned by Azure AD, Epiphan Connect assumes that the connection with your tenant remains valid.

Epiphan Connect uses its own application credentials to generate this token (no user-generated token or credentials are involved in this operation). No information from your Microsoft tenant is accessed as part of these checks.

Information stored by Epiphan Connect

Epiphan only keeps the minimum amount of information required for the functionalities of Epiphan Connect to work, to provide customer support, obtain usage statistics, and bill customers for the usage of the service. This section describes what information Epiphan Connect has access to, what information is collected by Epiphan, and the life cycle of that information in our systems.

What information is stored by Epiphan when using Epiphan Connect?

Below you can find the information Epiphan collects when you use Epiphan Connect:

- **Tenant information**: the name and unique ID of your tenant.
- **Meeting information**: the name of the meeting (if available), URL used to join the meeting, the audio mode selected (mixed or isolated), and the dates and times when Epiphan Connect was added and removed from the meeting.
  - The URL to join the meeting is only stored while Epiphan Connect is in use and is deleted from our servers when the Epiphan Connect instance is deleted.
- **Logs**: Any actions performed in Epiphan Connect during the meeting, as well as any changes in the status of the participants (when participants join, leave, enable their cameras and microphones, etc.), including usage statistics derived from those logs.

You can find more information on how Epiphan handles this information in our Privacy policy.

Media content in the meetings

Although Epiphan Connect can obtain the audio and video of the participants in the meeting, Epiphan does not record or store in any way any video, audio, chat messages, or any other type of content from any participant (user or application) in the call. Epiphan Connect just captures the audio and video of the stream selected by the user, upscales the media as needed, and sends it over SRT to the endpoints configured by the user.

Note that the systems receiving the SRT stream down the line might be able to record the stream.

Participants and their information

While Epiphan Connect is connected to a meeting, it has access to some basic information regarding the participants in the call. This includes:

- the name of the participant
- their unique ID
- what media they are sharing in the meeting
- if they are muted or not
- when they join and leave the call.

This information is kept in the Epiphan Connect instance that is connected to your meeting and is deleted when the Epiphan Connect instance is disconnected from the call.

No information from the participants is kept after the meeting, with the exception of the information compiled in the application logs.

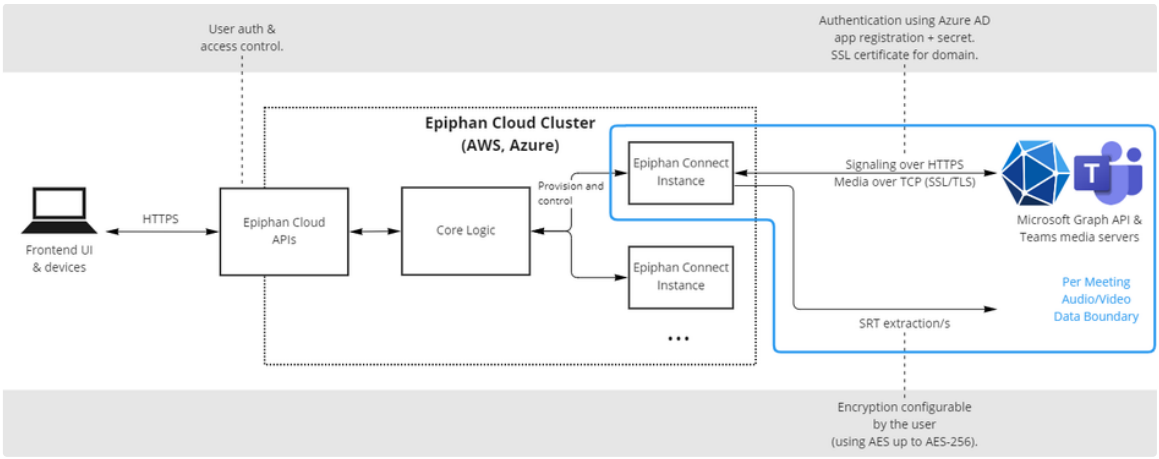
Architecture

When Epiphan Connect is scheduled to join a meeting, a new isolated instance of Epiphan Connect is created for your meeting. This instance will join the call, listen to changes in the status of the call and the participants, and perform the required media processing to output the selected streams as SRT feeds.

To do this, the Epiphan Connect instance needs to interact with several other components and services. This section describes how these components communicate with each other.

Diagram

Below you can find a diagram showing the main components of the Epiphan Connect service and how these components communicate with each other.



User secrets

Aside from the initial pairing process between Epiphan Connect and your Microsoft tenant, Epiphan Connect does not request, use, or store any secrets or credentials from your Microsoft tenant users. Instead, Epiphan Connect uses its own set of application credentials to generate the access tokens it needs to join the meetings in your Microsoft tenant.

During the pairing process between Epiphan Connect and your Microsoft tenant, Epiphan Connect checks that the person trying to pair the Microsoft tenant is an administrator in that tenant. To do this, Epiphan Connect asks the person to authenticate using their Microsoft user account. A short-lived token is generated during that authentication process that allows Epiphan Connect to check the permissions (or “claims“) that the user account has in the Microsoft tenant (see the User.Read permission in the ***What permissions are required for Epiphan Connect?*** section). This token is only used for this purpose and is not reused or stored in our systems.

Application credentials

In Epiphan Connect, long-lived credentials (Azure AD secrets, certificate passwords, etc.) are stored and managed through AWS Secrets Manager. All Epiphan Connect instances retrieve those secrets at runtime from the secrets manager service.

For short-lived credentials (i.e., valid only for the duration of the meeting) the credentials are created at the time the Epiphan Connect instance is created, and they are deleted once the instance is destroyed.

Epiphan Connect instances

Epiphan Connect instances are created as individual virtual machines. Each meeting runs on its own Epiphan Connect instance, isolated from other meetings.

All Epiphan Connect instances can be reached through the internet, but the only ports exposed are:

- Ports required to establish the SRT connections configured by the users (from 14000 to 14100).
- Ports required to communicate and exchange media with the Microsoft Graph APIs and Teams' media servers.

Threat Management

Vulnerability scanning

Epiphan executes weekly vulnerability scans to detect vulnerabilities in Epiphan's application. White box testing using Static Application Security Testing (SAST) tools are also used to analyze application source code to find vulnerabilities before deploying to production.

Availability and Reliability

Epiphan Connect and our cloud infrastructure are engineered for uninterrupted service and uptime with no degradation in performance.

Service Monitoring

Our engineering and customer success teams use industry-leading monitoring and alerting tools to visualize, analyze, and alert on metrics that could be impacting end users.

Organizational Security

Confidentiality Agreement

All Epiphan Employees are required to sign confidentiality agreement prior to onboarding.

Employee Security Training

All employees undergo regular security awareness training.

I'm a security researcher, and I found a vulnerability in Epiphan Connect. How do I report it?

Please contact us at admins@epiphan.com