Security and data privacy in Epiphan Connect

This document explains what information Epiphan Connect™ obtains from your Microsoft tenants or your Zoom accounts, their users, their meetings, and how Epiphan keeps that information secure.

Table of contents

- Permissions for Epiphan Connect in your Microsoft Teams tenant
  - What permissions are required for Epiphan Connect in Microsoft Teams?
  - Who can use Epiphan Connect in my Microsoft Teams meetings?
  - How can I revoke permissions for Epiphan Connect for Microsoft Teams?
  - Checking if the connection is still valid
- Microsoft Teams meetings created by Epiphan Connect
- Permissions for Epiphan Connect in Zoom
  - What permissions are required for Epiphan Connect to access the audio and video in a Zoom meeting?
  - What permissions are required for Epiphan Connect to join a meeting?
  - Who can use a paired Zoom user with Epiphan Connect in my meetings?
  - How can I revoke permissions for Epiphan Connect in Zoom?
- 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?

Permissions for Epiphan Connect in your Microsoft Teams tenant

In order for Epiphan Connect to be used in a meeting from 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 in Microsoft Teams?

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 Microsoft Teams 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 for Microsoft Teams?

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.

Microsoft Teams meetings created by Epiphan Connect

When using Epiphan Connect for Microsoft Teams the recommended approach is to schedule a Microsoft Teams meeting in your own organization so that you can have full control of this call. However, to do so you first need to complete a pairing process between your Epiphan Cloud team and the Microsoft Teams tenant that hosts the meeting.

If pairing your Microsoft Teams tenant is not possible, Epiphan Connect offers the option to create and host a Microsoft Teams meeting for you. These meetings have the following characteristics:

- Microsoft Teams meetings created in Epiphan Connect have an expiration time of 45 days, or until they are manually deleted in the Epiphan Cloud team.
- These meetings are associated with the Epiphan Cloud team in which they were created. For security reasons, only that associated team can join an instance of Epiphan Connect to the meetings.
- While the meetings are valid (i.e., they are not expired or deleted) anybody with the meeting URL can join them at any time. No waiting room or authentication requirements are enforced on people joining these meetings to make it easier for participants to join the call.
- Everybody joining these meetings will have permissions to share their camera, audio and screen.
- After the meetings are expired or deleted, no one can join these meetings again (they will be presented with a waiting room, and they won't be able to join in).

When creating a Microsoft Teams meeting using Epiphan Connect, we recommend to only share the meeting link with participants that you need to have in your call. It's not recommended to use these meetings for calls that don't involve the use of Epiphan Connect itself, or for calls where you need better control of the permissions of each participant, additional access control or any sort of privacy that is not covered by the characteristics listed above.

Permissions for Epiphan Connect in Zoom

When using Epiphan Connect in a Zoom meeting there are two types of permissions involved:

- Permissions to access the audio and video of the meeting participants (mandatory).
- Permissions to join meetings on behalf of a Zoom user (optional).

While Epiphan Connect doesn't require any permissions to connect to Zoom meetings that permit unauthenticated guests, it will require some permissions from the host of the call to access the audio and video of the participants while in the meeting. Without those permissions, Epiphan Connect cannot receive any media from the call.

In addition, if the meeting doesn't allow unauthenticated guest, Epiphan Connect might also require permissions to join using the identity of a Zoom user with access to that meeting.

This section describes these permissions, their scope, and how and when Epiphan Connect uses them.

What permissions are required for Epiphan Connect to access the audio and video in a Zoom meeting?

Once Epiphan Connect joins the Zoom call, it will wait for the host of the meeting to grant at least one of the following permissions. These need to be granted each time Epiphan Connect joins a meeting.

- **Permissions to do a live streaming**. These permissions give Epiphan Connect access to the raw audio and video of the participants in the call.
  - The content is only being streamed to the configured SRT destinations. No other streaming or recording of any kind is performed by Epiphan Connect.
  - When granted, the participants in the meeting should receive a notification telling them that Epiphan Connect has started a live stream.
- **Permissions to do a local recording**. Similar to the live streaming permissions, these will also grant Epiphan Connect access to the raw audio and video in the call.
  - Note that although the permission is described as “local recording“, Epiphan Connect won’t persist in any way or form any audio or video from the meeting. It will only stream the audio and video to the configured SRT destination.
  - When granted, the participants in the meeting will receive a notification telling them that Epiphan Connect has started a recording.

Depending on the configuration of the meeting and the Zoom account hosting it, only some of these permissions might be available in the call. Also, depending on the version of the Zoom client that the host is running, Epiphan Connect might try to request these permissions to the host directly (using a popup) or it will wait for the host to grant them manually.

In cases were none of these permissions can be granted by the host, the host also has the option to make the Epiphan Connect instance a host / co-host of the meeting. Doing so will automatically grant Epiphan Connect permissions to start receiving content from the call. The participants will still receive a recording / live streaming notification.

What permissions are required for Epiphan Connect to join a meeting?

If the Zoom meeting allows for unauthenticated guest to join, then no extra permissions are required for Epiphan Connect. Epiphan Connect can join the meeting as a guest.

If the Zoom meeting doesn’t allow for unauthenticated guests, then Epiphan Connect will require to use the identity of a Zoom user to join the meeting. To do this, you will first need to pair your Zoom user account to your Epiphan Cloud user or team. After completing the pairing process, you will be able to use Epiphan Connect in meetings using the identity of that Zoom user.

As part of the pairing process, Epiphan Connect will request you to approve the following permissions (i.e., “scopes“) for your Zoom user:

- **Basic information associated to your user account** (user_info:read): This allows Epiphan Connect to obtain some basic information to identify the user: name, picture and the Zoom generated IDs. This scope only grants access to the information of the user. Other users in the same Zoom account are not visible to Epiphan Connect.
- **Access to the user’s Zoom Access Key (ZAK)** (user_zak:read): This allows Epiphan Connect to join a meeting on behalf of this user.

You can pair Epiphan Connect to any Zoom user account (no admin-level permissions are needed). By default, the paired account is only visible to the Epiphan Cloud user that did the pairing, but you can share / un-share it with the rest of your Epiphan Cloud team in the settings page.

> **Note**: While any Zoom user can be paired, the recommended approach is to create a separate Zoom user in your Zoom account and then pair it with your Epiphan Cloud team. That way, you will be able to join Epiphan Connect to meetings in your account without having to pair any real user accounts.

Who can use a paired Zoom user with Epiphan Connect in my meetings?

When you pair a Zoom user in Epiphan Connect, that pairing is associated with the Epiphan Cloud team and user that did the pairing.

If the Zoom user is not shared with the Epiphan Cloud team, then only the Epiphan Cloud user that did the pairing can see it and use it to join meetings in Epiphan Connect. If the Zoom user is shared with the team, then anybody in the same Epiphan Cloud team as the user that did the pairing will be able to use it to join meetings in Epiphan Connect.

You might allow multiple Epiphan Cloud teams to use a Zoom user in Epiphan Connect, but to do so, you will need to repeat the pairing process for each individual team.

How can I revoke permissions for Epiphan Connect in Zoom?

The live streaming / local recording permissions granted to Epiphan Connect are only valid during the time that Epiphan Connect is connected to the meeting. When Epiphan Connect is disconnected from the call or the Zoom meeting ends, Epiphan Connect automatically loses these permissions.

The host of the meeting can also revoke these permissions manually during the call or simply disconnect Epiphan Connect from the meeting.

> **Note**: We don’t recommend removing Epiphan Connect from inside the Zoom UI. Any participants removed in that way (including Epiphan Connect) won’t be able to join the Zoom meeting again. Instead, we recommend disconnecting Epiphan Connect from the call in the Epiphan Connect UI.

As for **the Zoom users paired to Epiphan Connect**, you can 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 Zoom user from this team.

You can also revoke the permissions granted to the Epiphan Connect application by going to https://marketplace.zoom.us/user/installed and clicking **Remove** on the Epiphan Connect app. Note that no Epiphan Cloud team will be able to use your Zoom user in Epiphan Connect to join meetings after these permissions are revoked (the user will be listed as *deauthorized* in those teams).

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

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

Microsoft tenant information

If you choose to pair your Microsoft Teams tenant with Epiphan Connect, Epiphan will collect the follow information about the tenant:

- The name of the tenant, as shown in Azure Active Directory.
- The unique ID of your tenant.

This information is kept in our databases as long as the pairing exists and is deleted when this pairing is removed from the Epiphan Cloud team.

Zoom user information

If you choose to pair your Zoom user with Epiphan Connect, Epiphan will collect the following information about the user:

- The name of the user, as shown in Zoom.
- The URL of the profile picture for the user.
- The unique ID of the user and account.
- The access tokens and refresh tokens to obtain the information of this user from Zoom's APIs.

This information is kept in our databases as long as the pairing exists with at least one Epiphan Cloud team. When the pairings are removed, the information of the user is deleted from the database. For additional security, the name, picture URL and tokens are also encrypted before being stored using AES-256.

Meeting information

When you start Epiphan Connect to join it to a meeting, Epiphan will collect the follow information about that meeting:

- The name of the meeting, if available.
- The URL used to join the meeting.
- The unique ID of the meeting. For Zoom meetings, this is the meeting number. For Microsoft Teams meetings, this is the thread ID.
- The passcode for the meeting, if provided (for Zoom meetings only).
- The audio mode selected (mixed or isolated).
- The dates and times when Epiphan Connect was added and removed from the meeting.

The meeting URL, unique ID and passcode are only stored in our databases while Epiphan Connect is in use and are deleted from our servers when the Epiphan Connect instance is deleted. For additional security, these values are also encrypted before being stored using AES-256.

Logs

Epiphan collects logs in order to find, analyze and solve any problems that might occur in Epiphan Connect, as well as to provide better support for our customers and generate usage statistics on how people are using our products.

These logs include any actions performed in Epiphan Connect during the meeting, any changes in the status of the participants (when participants join, leave, enable their cameras and microphones, etc.), as well as configuration settings used in Epiphan Connect.

To minimize the presence of sensitive information in our logs, Epiphan Connect applies to following treatment to the information before writing it to our logging systems:

- Names of participants in the meeting are reduced to only their initials (e.g., "John Doe" is reduced to "J.D."). This makes it so that each individual participant is different enough from others in the context of a meeting, while still being impossible to identify based on just the logs. Using initials also allows our support team to find logs related to a particular participant if a customer reports having issues with a specific person in a meeting (e.g., "John Doe's video was dropping frames").
- Passphrases used when configuring SRT outputs are removed before logging these settings.

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 IDs (for Microsoft Teams meetings only).
- 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.

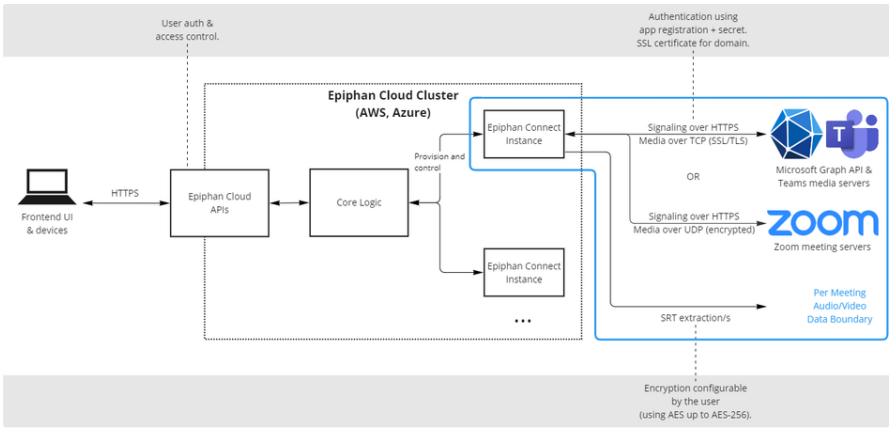
Architecture

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

Epiphan Connect uses its own set of application credentials to generate the access tokens it needs to join the meetings in your Microsoft tenants and Zoom accounts. However, if you choose to pair your Microsoft tenant or your Zoom account to Epiphan Connect, there are other tokens that are involved as part of this process.

User secrets for Microsoft Teams

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.

Aside from that 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.

User secrets for Zoom

When you pair a Zoom user account with Epiphan Connect, there are a few tokens that are generated as part of the pairing process. These secrets allow Epiphan Connect to maintain access to the paired Zoom user to generate the tokens needed to join your meetings. Below you can find more information about each token:

- **Access token**: This is a short-lived token (~1 hour) that is used to obtain both the information of the user (name, picture and IDs) during the initial pairing process, as well as obtaining the Zoom Access Key (ZAK) on demand, when you use the user account to join a meeting in Epiphan Connect. As a short-lived token, this token is cached in our systems and is not stored in our databases.
- **Refresh token**: This is a long-lived token that allows Epiphan Connect to obtain new access tokens when needed (which in turn are needed to obtain the ZAK tokens). These tokens are encrypted using AES-256 and stored in our databases.
- **Zoom Access Key (ZAK)**: This is a short-lived token (~5 minutes) whose sole purpose is to allow Epiphan Connect to join a meeting on behalf of the Zoom user. Given their short duration, these tokens are requested when needed (using the access token) and are not stored or cached in our systems.

Short lived tokens (i.e., the access token and ZAK) are automatically expired and deleted from our systems. Long lived tokens (i.e., the refresh token) are stored in our systems for as long as the Zoom user account is paired with a Epiphan Cloud team. If all pairings with the Zoom user account are removed, the account is deleted from our database.

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.

- Ports required to communicate and exchange media with the Zoom meetings and 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