

CONNECTIVITY FAQ FOR IT

Introduction

This page is geared towards the IT department of Eddyfi Technologies product customers. The Eddyfi Technologies products rely on Internet connectivity for some core functionalities (licensing) and for ease of life and productivity enhancing functionalities (support, online storage, teleconference access, etc.).

Eddyfi Technologies develops and tests these functionalities at the highest security standards and is a certified provider when applicable.

In order to allow users to enable the full power of their devices, some IT policy configuration might be necessary.

If you are the end user of Eddyfi Technologies products, please forward this page to your IT department to assist them in enabling the full potential of your devices.

Enterprise Network Access

Device Information

Eddyfi Technologies devices run Windows 10 in a locked-down environment, restricting user-level access to the underlying operating system. The Cypher system runs on Windows 11.

Device Hostname

The hostname can be found in the connectivity page in the product software.

Device MAC Address

The device MAC address can be found on a sticker underneath the instrument.

Access Requirements

Wi-Fi

Eddyfi Technologies systems currently support WPA2-Personal (PSK) and WPA2-Enterprise (802.1X) networks. WPA3 is not supported as of now. The Eddyfi Technologies systems have the capability to interact with captive portals.

To ensure that Eddyfi Technologies systems can connect to your enterprise WPA2 network, please make sure the Wi-Fi SSID is visible.

Ethernet

Static IP addresses are not supported by the system. The device requires an IP address assigned automatically via DHCP.

To enable the system to connect to your enterprise network:

- Ensure DHCP is Enabled
- If MAC address filtering is enforced
- Add the instrument MAC address to the allowlist or assign a static DHCP reservation.

Licensing

How Does It Work?

The Eddyfi Technologies products use the Zentitle Nalpeiron online licensing system.

- For activation, the software accesses an endpoint to inform the Nalpeiron backend that it is now the holder of this licence.
- It is a node lock-type licence - once it is acquired by a given system, it needs to "call home" once a year to the Nalpeiron online service to stay active - it does not require constant internet access.
- As a node lock license, on desktop systems it can be transferred using the Release functionality, then activated on a different computer. This process requires internet access by both computers.

Access Requirements

The following endpoint URLs should be whitelisted:

- eddyfi.nalpeiron.com
- eddyfinsa.nalpeiron.com
- my.nalpeiron.com


Over The Air Updater

How Does It Work?

An Eddyfi Technologies cloud service allows the products to check whether new software versions are available and download and install them automatically.

Access Requirements

This functionality is hosted on Microsoft Azure. The following domains must be whitelisted to allow it to work:

- login.microsoftonline.com (port 443)
 - microsoftonline.com (port 443)
 - azurewebsites.net (port 443)
- 

Online Storage

How Does It Work?

Previan is a Microsoft Publisher Verified application provider that developed the Eddyfi OneDrive Integration app, which complies with the Publisher Verification Program. It allows users to use a personal or enterprise Azure Active Directory account to log in to synchronize inspection files from their instrument to a folder within their OneDrive account.

The app only reads and writes to this specific “Eddyfi” folder.

Access Requirements

Required Microsoft Graph API Permissions

- Files.ReadWrite – Delegated – Full access to user's OneDrive files
- User.Read – Delegated – Sign in and read user profile

Admin Steps to Enable the Application

Entra Policy

1. Go to Microsoft Entra Admin Center.
2. Navigate to: Microsoft Entra ID > Enterprise applications > User settings.
3. Under 'User consent for applications', select: 'Allow user consent for apps from verified publishers...'
4. (Optional) Set up Admin Consent Workflow for approval requests.
5. (Optional) Manually register the app and pre-consent to required permissions:
 1. Microsoft
 2. Input app details (name: Eddyfi OneDrive Integration).
 3. Go to Permissions and grant admin consent for Files.ReadWrite and User.Read.

Endpoint Whitelist

Microsoft Identity and Authentication (Azure AD / Entra ID)

Used for login and consent.

- <https://login.microsoftonline.com>

- <https://aadcdn.msftauth.net>
- <https://aadcdn.msauth.net>
- <https://secure.aadcdn.microsoftonline-p.com>
- Port: 443 (HTTPS)

Microsoft Graph API

Used to access user profile and OneDrive files.

- <https://graph.microsoft.com>
- Port: 443 (HTTPS)

OneDrive and SharePoint Online

Used if the app interacts with or embeds content from OneDrive or SharePoint.

- https://*.sharepoint.com
- https://*.onmicrosoft.com
- https://*.onedrive.com
- https://*.office.com
- Port: 443 (HTTPS)

Microsoft Consent Experience and Static Content

Used for login UI elements, branding, and security tokens.

- <https://consent.microsoftonline.com>
- <https://login.live.com>
- https://*.msidentity.com
- https://*.microsoftonline.com
- Port: 443 (HTTPS)

Notes on Firewalls and DPI (Deep Packet Inspection)

- SSL inspection can break authentication tokens. Ensure these domains are exempt from SSL decryption if DPI is in use.



- All traffic is encrypted via HTTPS over port 443.

Teleconference

How Does It Work?

As part of the Customer Success Program, Eddyfi Technologies users have the capability to start a Zoom teleconference session from their instrument to give a colleague or Eddyfi support the ability to see the screen and control the instrument remotely.

Access Requirements

The following domains should be whitelisted:

Domains to Whitelist	Ports
zoom.us, *.zoom.us, api.zoom.us, zoom.us/oauth/*	443 (HTTPS)
source.zoom.us, zoom.us/wc/*, *.cloudfront.net, *.zoomcdn.io	443 (HTTPS)
zoom.us, zoomcloudpbx.com	8801–8810 UDP, fallback on 443/8443
wss://ws.zoom.us	443 (WSS)

Exclusions

As per Eddyfi Technologies' contractual obligations with Zoom, this service is not available in the following countries: China, Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan



Eddyfi App

How It Works

The Eddyfi mobile app is available on both Android and Apple stores. It connects to Eddyfi embedded devices either directly using the device's Wi-Fi hotspot or through a Wi-Fi network if both devices are connected to that same network.

Access Requirements

If both devices are allowed to connect to a given Wi-Fi network, there are no additional requirements. If either of the devices is not allowed to connect, it is better to disconnect both so that the mobile app can connect directly to the embedded device without attempting to go through the network.

If the Wi-Fi network has **client device isolation** enabled, the mobile app and the embedded device will not be able to discover or communicate with each other even if both are connected to the same network. In such cases, they must be in **physical proximity** to establish a direct connection.

Send Problem Details

How It Works

When a customer is in contact with Eddyfi Technologies for technical support, they may be asked to send the problem details. These include problematic files.

Access Requirements

This functionality is hosted on Microsoft Azure. The following domains must be whitelisted to allow it to work:

- login.microsoftonline.com (port 443)
- microsoftonline.com (port 443)
- azurewebsites.net (port 443)



Insights

How It Works

If the Eddyfi Technologies product has accepted to be part of the Product Improvement Program, usage metrics will be sent to help Eddyfi improve and keep the product as fit for operation as possible.

The metrics are compliant with all applicable laws and are anonymized at the source.

It uses Azure App Insights.

Access Requirements

The following endpoint needs to be whitelisted: <https://dc.services.visualstudio.com>, port 443 (HTTPS)

