DVB-NIP ANALYZER

Start analyzing DVB Native IP

Install the analyzer, create and manage analysis contexts, inspect services, configure telemetry, and understand the available tests.

ORIENTATION

1. What is DVB Native IP?

DVB Native IP, or DVB-NIP, delivers IP-based media and data over a DVB broadcast network. Instead of delivering only traditional television channels, DVB-NIP transports services, manifests, files, and signalling that can be consumed directly by IP applications.

The DVB-NIP Analyzer reads a live network interface, a packet capture (PCAP), a transport stream file, or an Inverto QStream input. It can show announced services, inspect the NIP signalling tree and object carousels, monitor bitrate, retain service objects, record packets, and run in-app conformance checks.

> **Before you begin**
>
> You must have access to a DVB-NIP stream, either as a recorded PCAP file, an MPE transport stream file, or multicast IP packets carrying a DVB-NIP stream on your network. PCAP samples can be downloaded from the DVB-NIP V&V web page.

Four terms to know

Analysis context A configured DVB-NIP source together with its analysis settings. Each context is analyzed independently and stores its own results.	**Service** A media service discovered in the DVB-NIP stream, typically a live TV service delivered using DASH or HLS. Joining a service retains its files and manifests in the analyzer cache. Monitoring opens a playback view when the service exposes a playable manifest.
Carousel A collection of files and signalling information that is repeatedly broadcast. Because the content is transmitted continuously, a receiver can start receiving it at any time.	**Recording** A packet capture (PCAP) of the analyzed traffic.

INSTALLATION

2. Install the analyzer

Use a Windows 10 or Linux system with an Intel i5 processor or equivalent, at least 8 GB of RAM, and 200 MB of free disk space. Linux installation also requires Docker.

Windows

1. Download the DVB-NIP Analyzer ZIP archive from the public DVB Verification & Validation page.
2. Extract the ZIP archive.
3. Double-click `dvb-nip-analyzer.exe` to start the application.

> ⚠ **Run one instance only**
> Only one instance of DVB-NIP Analyzer can run at the same time.

Linux with Docker

Pull the latest analyzer image. See DVB-NIP Analyzer on Docker Hub for the current image and tags.

```
docker pull sessystems/dvb-nip-analyzer
```

To receive multicast UDP/IP streams through the host network, run the container with host networking:

```
docker run --rm --net=host --name=dvb-nip-analyzer
              sessystems/dvb-nip-analyzer
```

If host network access is not needed, publish port 8000 for the web interface:

```
docker run -p 8000:8000 --rm sessystems/dvb-nip-analyzer
```

To analyze PCAP or transport stream files, make them available to the DVB-NIP Analyzer container by mounting a host directory as read-only. For example, if you have a `samples` directory in your current working directory, run:

```
docker run --rm --net=host -v "$PWD/samples:/samples:ro"
              sessystems/dvb-nip-analyzer
```

In **PCAP file path** or **Transport stream file path**, enter the path inside the container, such as `/samples/example.pcap`.

Open `http://localhost:8000` in your browser after the container starts.

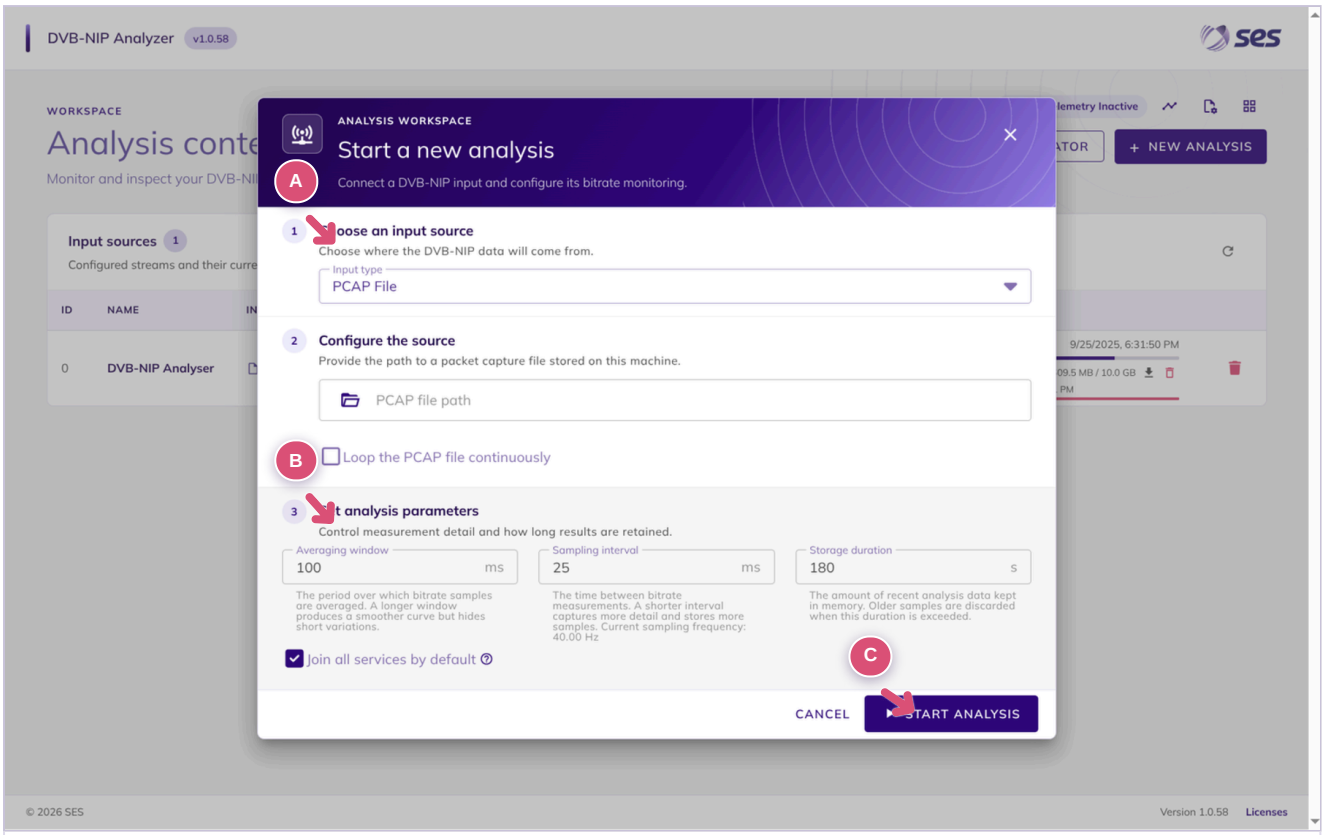
WORKFLOW 1

3. Create an analysis context

1. Select **New Analysis** on the **Analysis contexts** page.
2. Under **Choose an input source**, set **Input type** to **PCAP File**, **TS File**, **Inverto QStream**, or **Network Interface** when available.

3. Complete **Configure the source**.

4. Review **Set analysis parameters**, then select **Start analysis**.



A Choose the input and configure its source.
B Review the analysis parameters.
C Select Start analysis.

Join a live stream

There are two ways to receive a live multicast stream:

> **The first way is not available on Windows**
> Direct connection to the multicast network is available only when running the analyzer in a Linux container. Using an Inverto QStream remains available on Windows.

1. **Connect directly to the multicast network.** The analyzer must have access to a network that transports the multicast IP packets. When creating the analysis, select **Network Interface** as the input type, then choose the network interface connected to that network.

2. **Use an Inverto QStream.** Select **Inverto QStream** as the input type, enter the QStream IP address, then provide tuning query parameters using SAT>IP syntax. Include `mcast_in=all` to receive all IP packets.

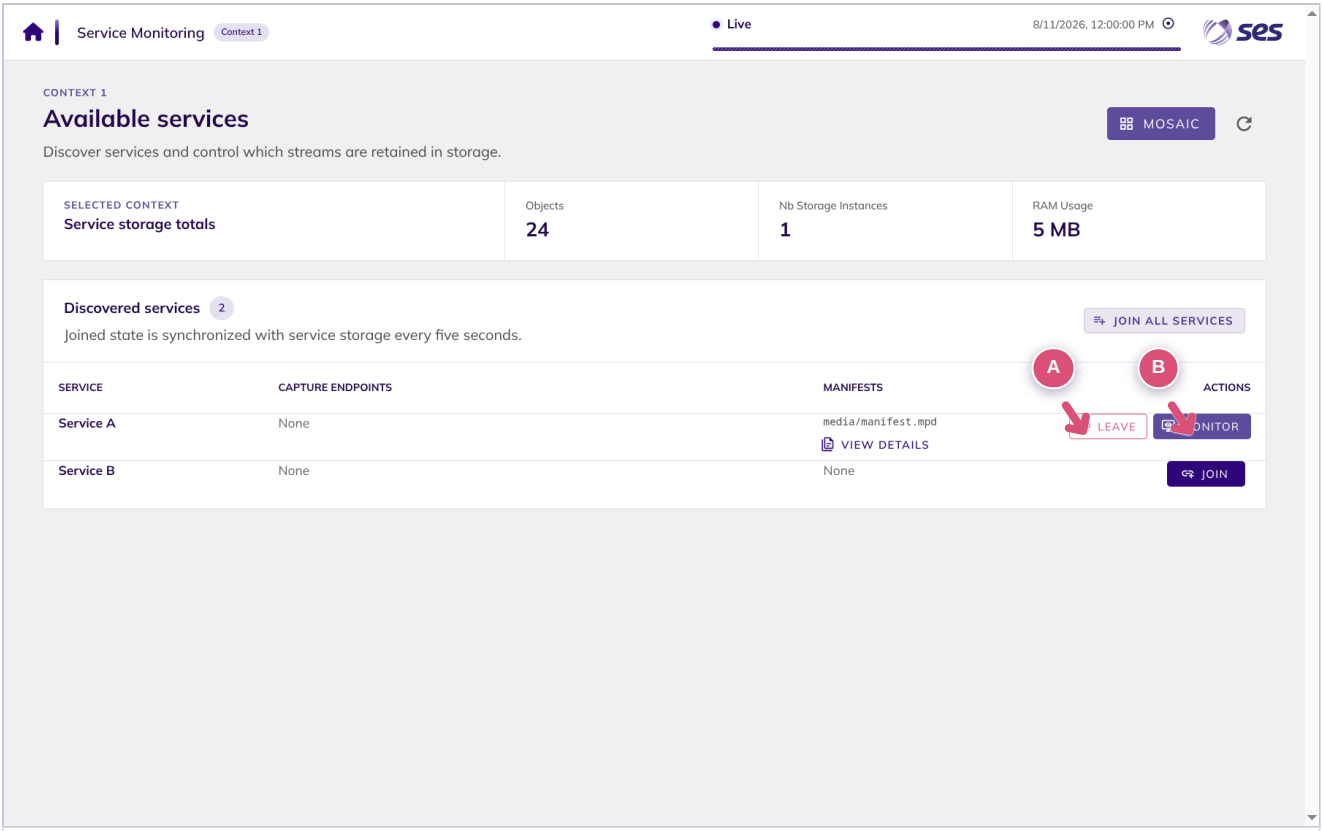
For example:

```
http://qstream-ip/?
freq=11141&orb=192&pol=h&msys=dvbs2&sr=23500&mcast_in=all
```

WORKFLOW 2

4. Join and monitor a service

1. Find your context and select **Services** under **Analysis views**.
2. In **Discovered services**, select **Join** for one service. Joining retains that service's objects in storage.
3. **Monitor** becomes available only after the service has been joined and a playable DASH or HLS manifest has been discovered. Select **Leave** to stop retaining the service.
4. Use **Join all services** or **Leave all services** only when you intend to change every discovered service in the context.



A Leave a joined service when you no longer need retained objects.

B Monitor is available only for joined playable services.

WORKFLOW 3

5. Configure a packet recording

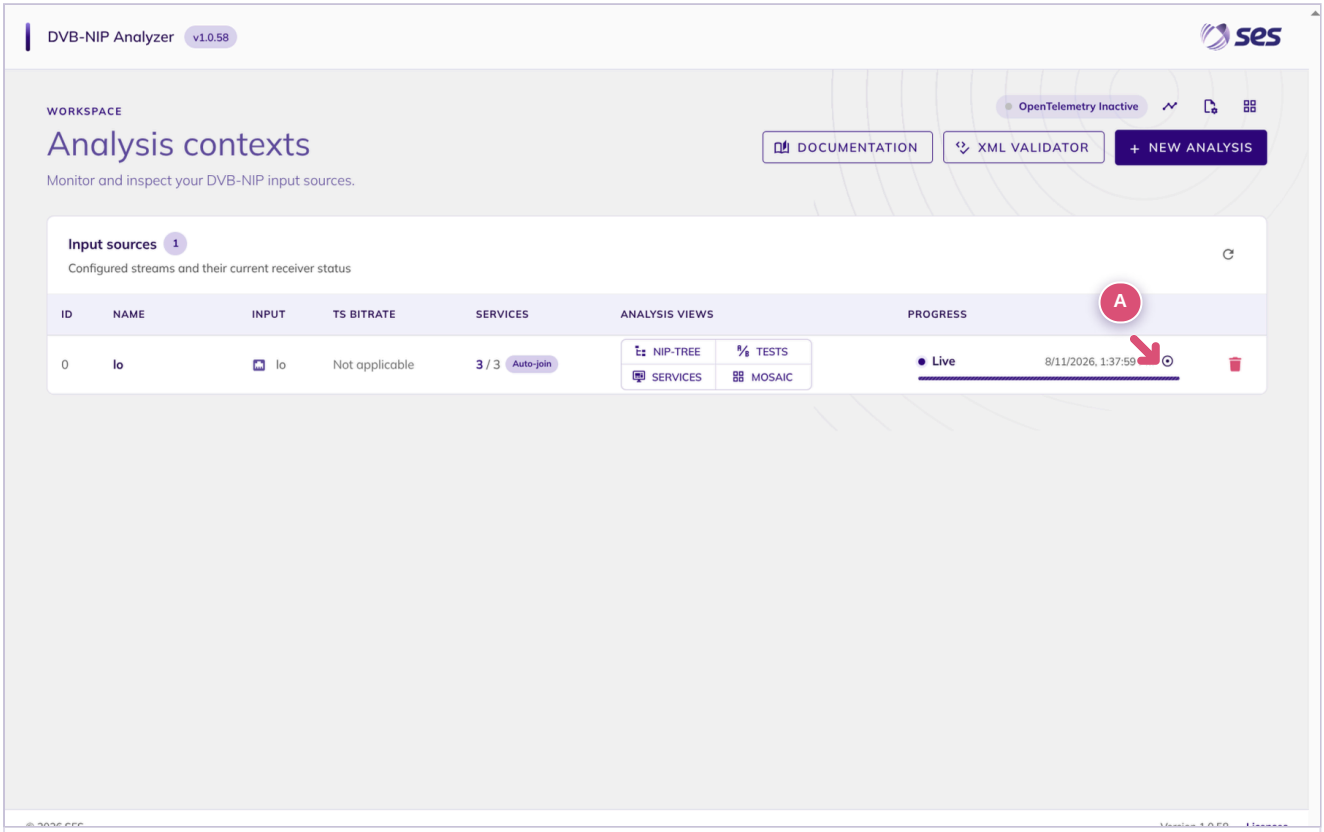
1. In a context row, first select the record button labelled **Configure packet recording**. The configuration dialog opens.
2. Choose **Continuous** or **Stop at limit**.
3. Set **Maximum duration** and **Maximum size**.
4. Select **Start recording**.
5. Use **Download recording snapshot** to save a PCAP, or **Remove packet recording** to stop and remove it.

Continuous

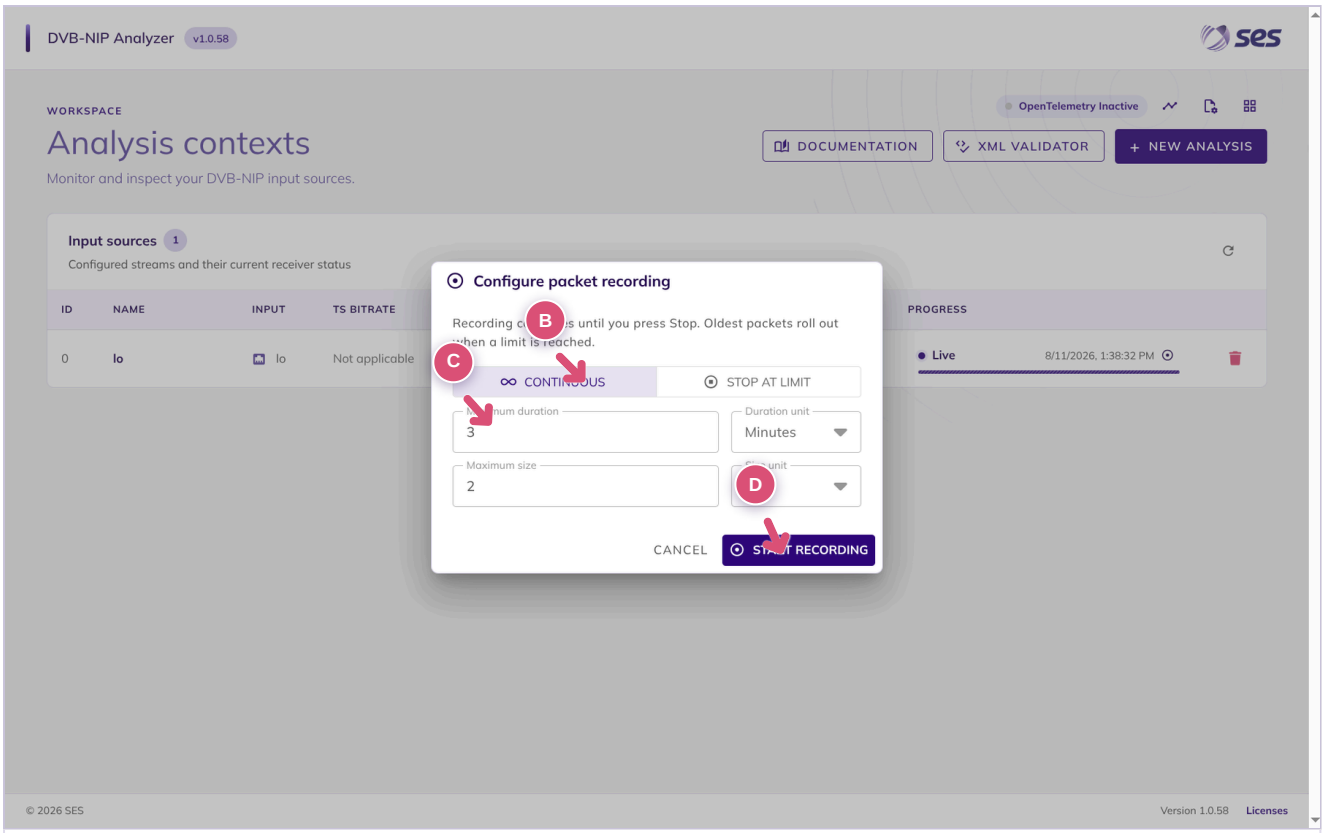
Recording continues until you remove it. When either configured limit is reached, the oldest packets are evicted so newer packets can roll in.

Stop at limit

Recording stops as soon as the first limit is reached: maximum duration or maximum size. Recording can also be stopped manually before a limit is reached.



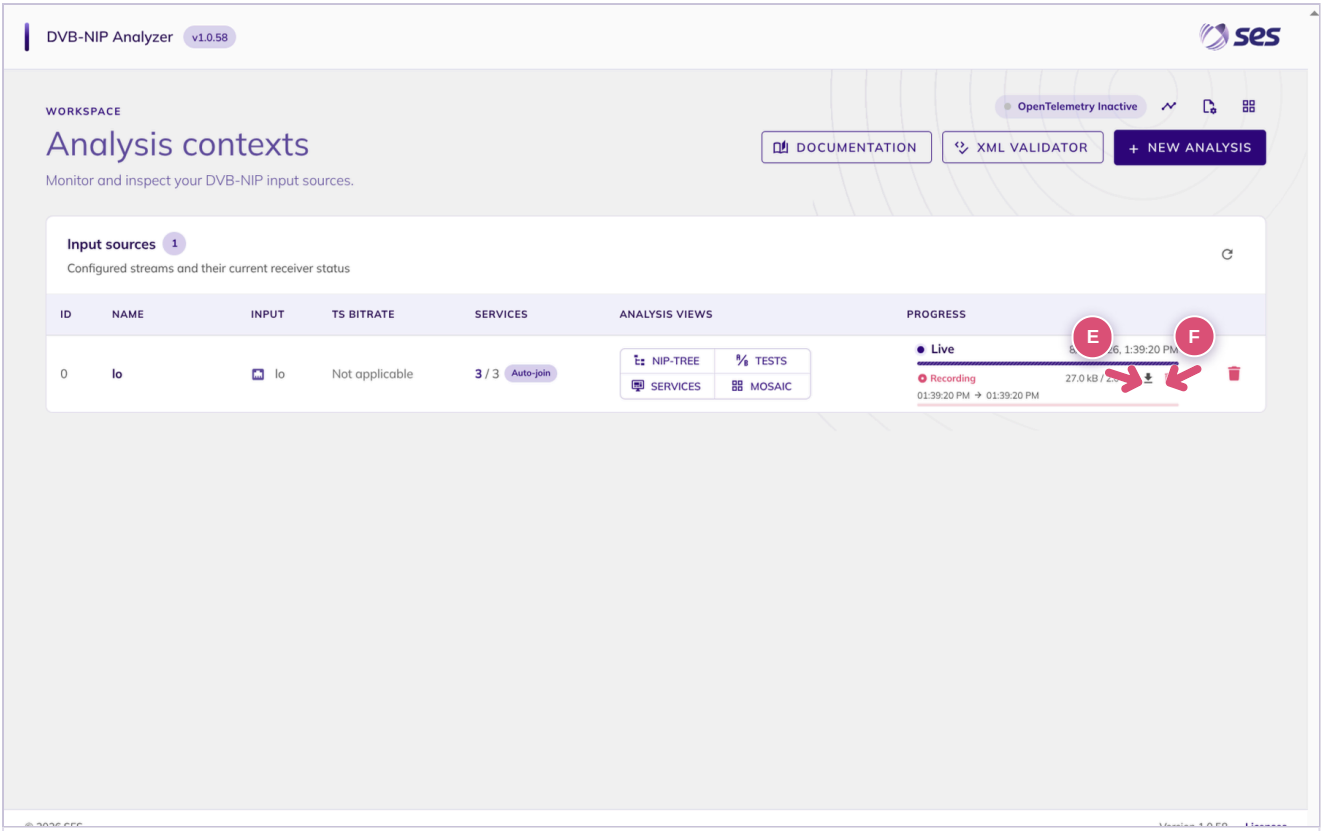
A Select Configure packet recording in the context row.



B Select Continuous or Stop at limit.

C Set Maximum duration and Maximum size.

D Select Start recording.



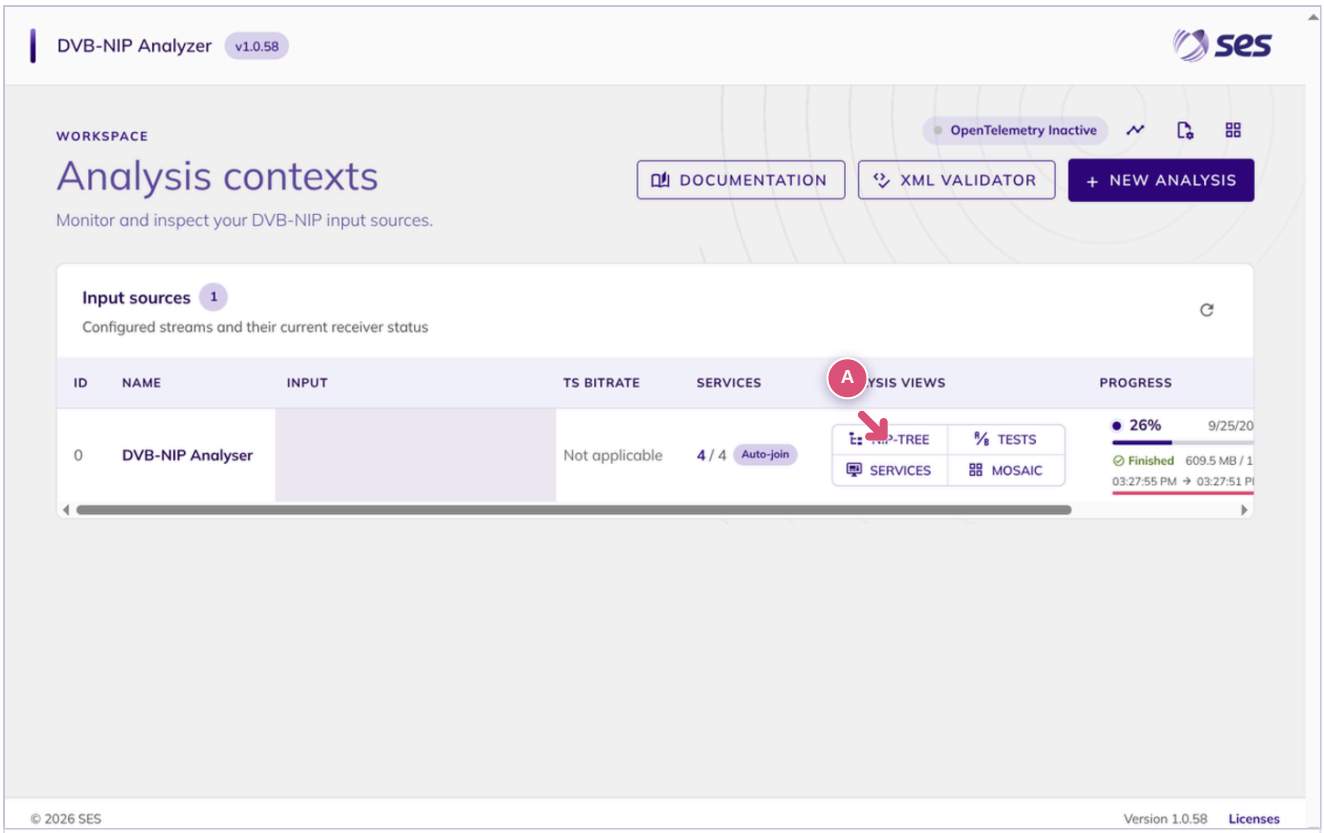
E Download the current recording snapshot.

F Stop and remove the packet recording.

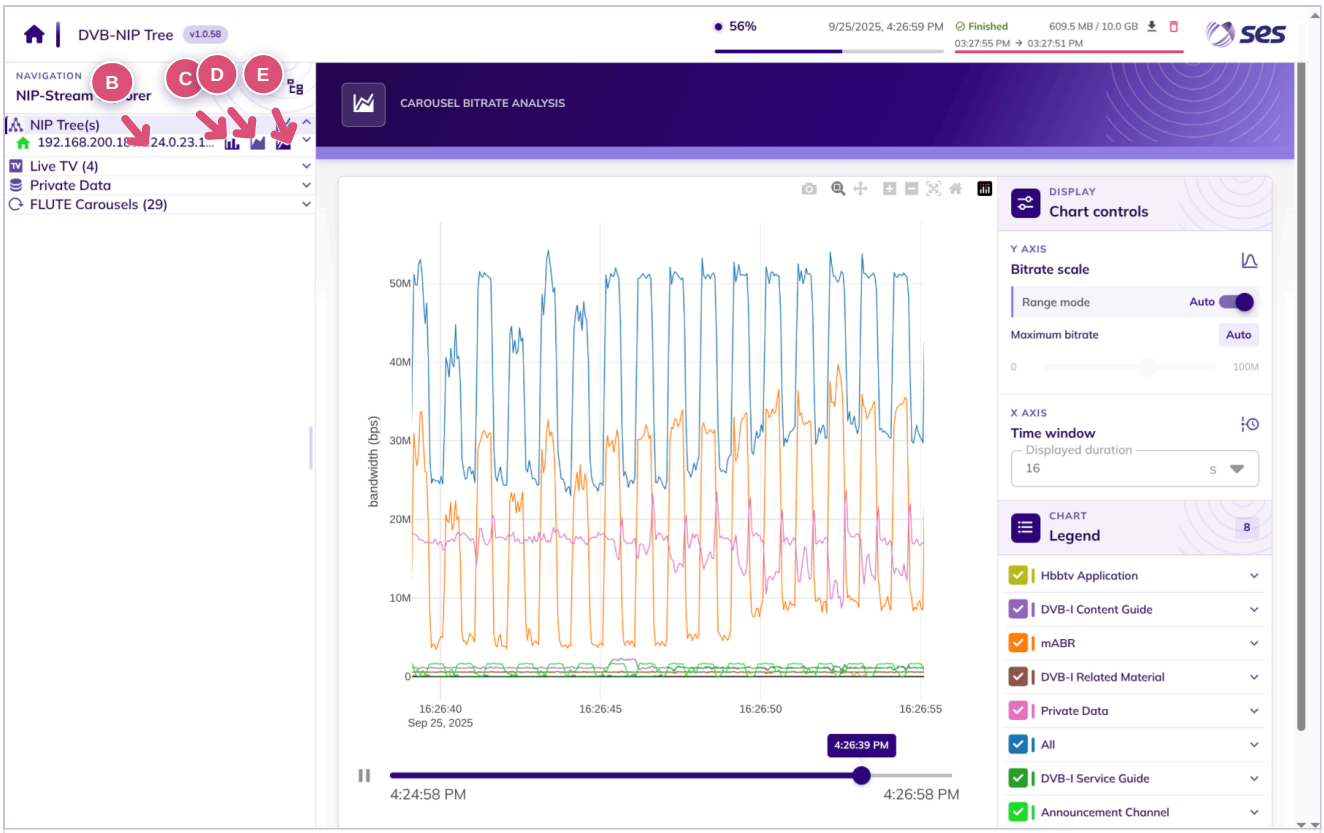
WORKFLOW 4

6. Open and navigate the NIP tree

1. Find your context and select **NIP-Tree** under **Analysis views**.
2. Use the **NIP-Stream explorer** sidebar to expand signalling nodes, transport sessions, multicast sessions, and their files.
3. On a carousel row, use **Open Statistics for this carousel**, **Open bitrate analyzer for this carousel**, or **Open bitrate analyzer for this tree** when available.
4. Drag the sidebar divider to give long node names more room.



A Select NIP-Tree from Analysis views in your context row.



B Use the NIP-Stream explorer to expand nodes and sessions.

C Open Statistics for this carousel. **D** Open bitrate analyzer for this carousel.

E Open bitrate analyzer for this tree.

WORKFLOW 5

7. Watch joined services in Playback Mosaic

Playback Mosaic shows the **Joined channel mosaic**, where each available tile automatically starts live playback and displays playback health indicators.

> ⓘ **Before you begin**
>
> Join at least one service that exposes a playable DASH or HLS manifest. Without a joined playable service, Mosaic remains unavailable or empty.

1. Open **Playback Mosaic** from a context or from the application navigation after joining a playable service.

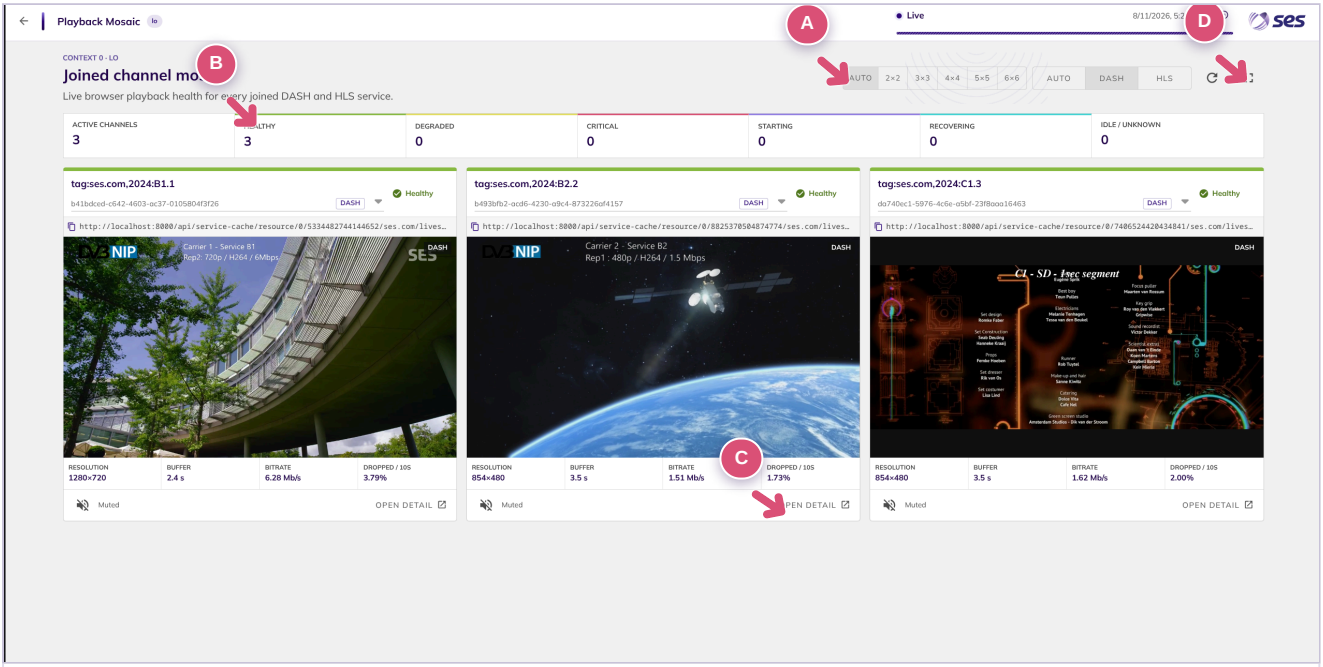
2. Choose grid density **Auto, 2×2, 3×3, 4×4, 5×5, or 6×6** and, when useful, choose protocol preference **Auto, DASH, or HLS**.

3. Watch each available tile begin live playback automatically. Use its health and metrics to check playback; if a tile offers more than one manifest, choose the source in its manifest selector.

4. Select **Listen to this channel** for one tile at a time, or select **Open detail** for that service's full playback monitor.

5. Select **Enter wall mode**. Wall mode still opens inside the page if browser fullscreen is denied, so browser fullscreen is not guaranteed.

6. Select **Exit wall mode** to restore the normal controls.



A Choose grid density and playback protocol when useful.

B Check live playback health, metrics, and manifest choice.

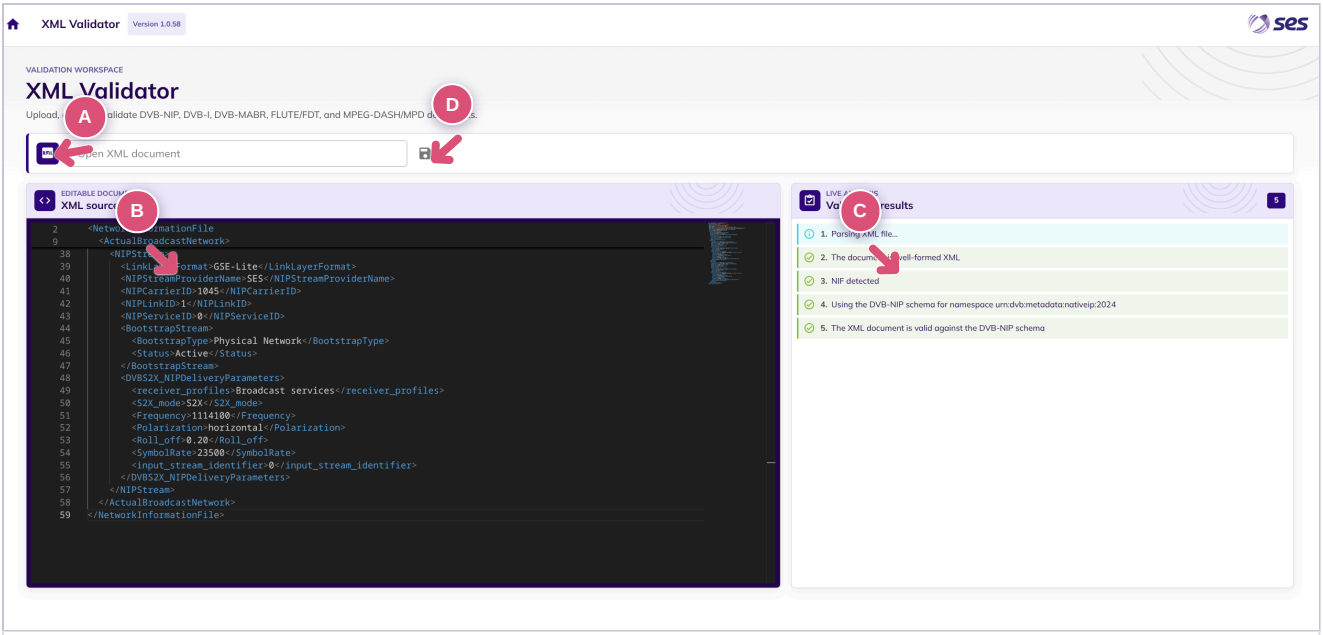
C Listen to one channel or Open detail.

D Enter wall mode.

VALIDATION

8. Validate an XML document

Select **XML Validator** on the **Analysis contexts** page to upload, edit, and validate **DVB-NIP**, **DVB-MABR**, **DVB-I**, **FLUTE/FDT**, and **MPEG-DASH MPD** documents. The validator automatically detects and selects the appropriate XML schema and displays results alongside the XML, which can be downloaded after editing.



A Open an XML document. **B** Edit the XML source.

C Review the live validation results. **D** Download the edited document.

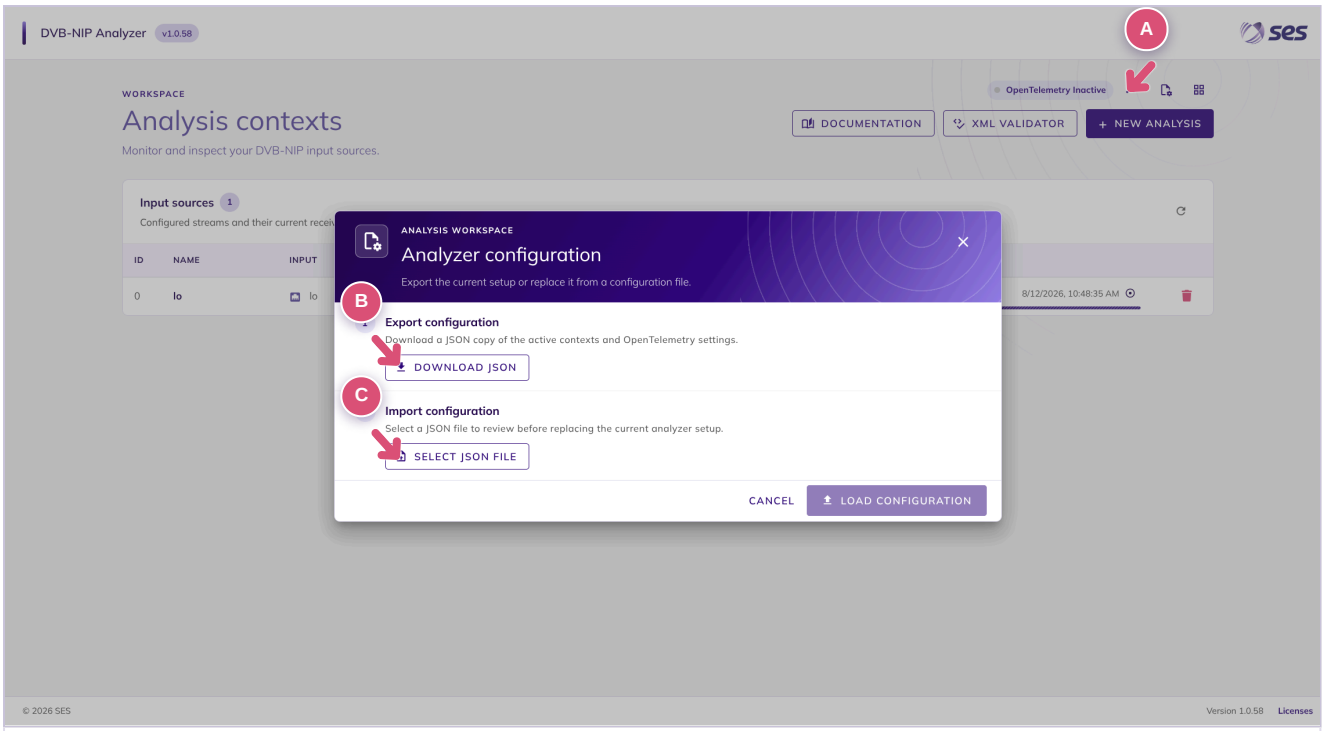
WORKSPACE MANAGEMENT

9. Save and load analyzer configuration

Open **Analyzer configuration** from the configuration button on the **Analysis contexts** page. An exported configuration contains the active analysis contexts and the current OpenTelemetry settings.

1. Under **Export configuration**, select **Download JSON** to save the current setup.
2. To restore a saved setup, select **Select JSON file** under **Import configuration** and choose a valid configuration file.
3. Review the displayed configuration version, analysis context count, and OpenTelemetry status.
4. Select **Load configuration** to apply the reviewed file.

> ⚠ **Loading replaces the current setup**
>
> Export the current configuration before loading another file. If loading fails after replacement begins, existing contexts may already have stopped and are not restored automatically.



A Open Analyzer configuration. B Download the current setup as JSON.

C Select a JSON file, review it, then load it.

OBSERVABILITY

10. Configure OpenTelemetry

OpenTelemetry sends analyzer traces, metrics, and logs to an observability platform. Enable it for long-term monitoring, integration with existing dashboards and alerts, and easier investigation when issues occur.

The status indicator reports whether telemetry is currently **Active** or **Inactive**.

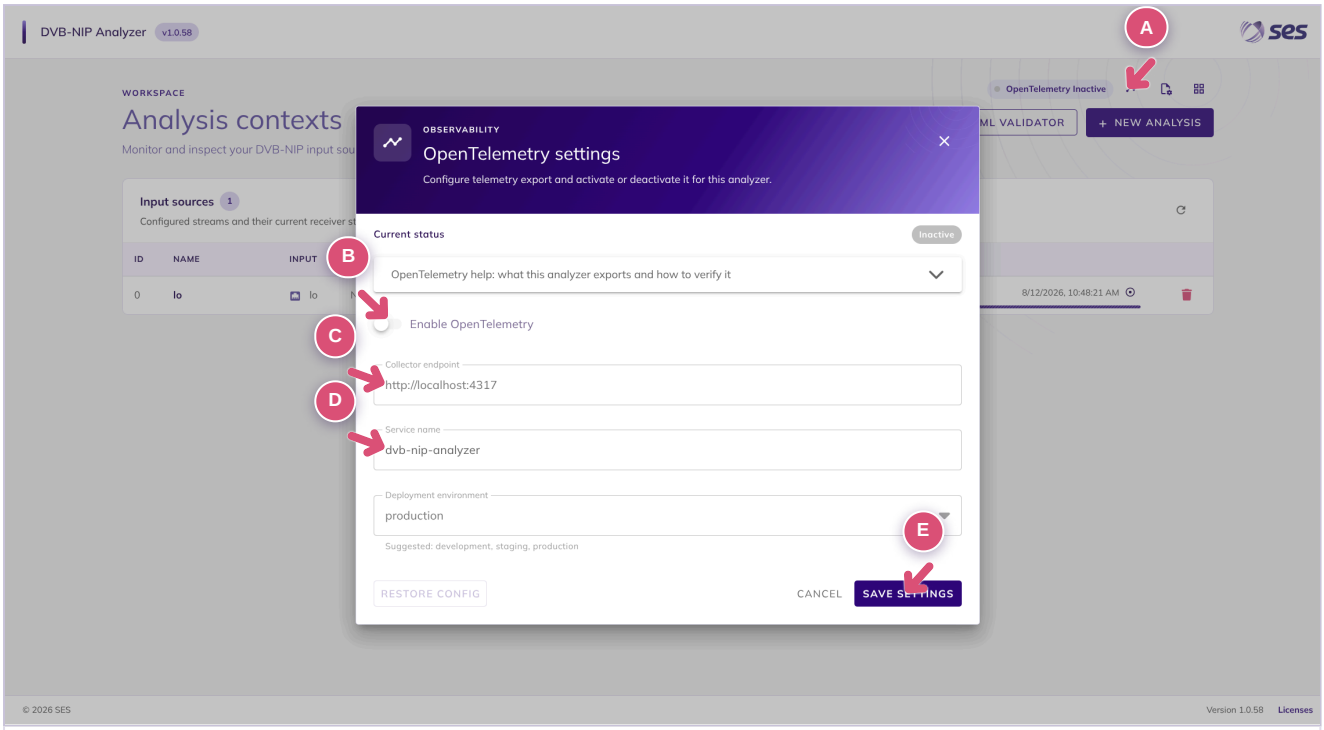
1. Open **OpenTelemetry settings** from the telemetry settings button on the **Analysis contexts** page.

2. Toggle **Enable OpenTelemetry** to activate or deactivate telemetry export. A **Collector endpoint** is required when OpenTelemetry is enabled.

3. Enter the collector's OTLP/gRPC address in **Collector endpoint**, such as `http://localhost:4317`.

4. Set **Service name** to identify the analyzer in telemetry backends and **Deployment environment** to identify its environment.

5 Select **Save settings** to apply the values.



A Open OpenTelemetry settings. B Enable or disable telemetry export.

C Set the Collector endpoint. D Set Service name and Deployment environment.

E Save settings.

VERIFICATION

11. Run and export automated tests

In-app DVB-NIP Test Suite

Select **Tests** for a context. The analyzer loads the current DVB-NIP tree, runs its conformance checks, and reports totals, errors, warnings, progress, and individual results. When progress reaches 100%, **Export to Excel** downloads **dvb-nip-analyzer-result.xlsx** with the current report.

The suite tests a limited set of points from the DVB-NIP standard. Because the standard is complex and supports many use cases, the suite cannot cover every scenario and bugs may still exist.