Network Dataflow Analyzer (NDA) Pro

Getting Started and User Guide

Product version	0.88.3
Last updated	2025-12-13
Applies to	NDA Desktop (Electron) and NDA Web Viewer (browser)
Notes	The guide filename may contain an older version number; check Settings (footer) for the authoritative app version.

Tip: This document includes a clickable outline on the next page.

Table of Contents

Click a section to jump there. (In Word, you can still insert an automatic TOC if you prefer.)

About this guide

Filename note: This guide's filename may include an older version number (for example v0.41.1). The authoritative app version is shown in NDA under Settings (footer) and in the application packaging.

This guide is intentionally detailed and written for:

- SOC analysts and incident responders
- OT engineers (plant / ICS / SCADA environments)
- IT/network engineers doing post-capture investigation
- Administrators who deploy NDA and support its workflows

Conventions used in this guide:

- Menu paths are written like Settings -> License or Settings -> Exports.
- Keyboard shortcuts are written like Ctrl/Cmd+Shift+E (Windows/Linux uses Ctrl, macOS uses Cmd).
- "Desktop" means the Electron application. "Web Viewer" means the browser build.
- "PCAP" means .pcap or .pcapng unless stated otherwise.

1. Overview

Network Dataflow Analyzer (NDA) turns packet captures into an interactive network graph so you can answer:

- What talked to what?
- When did it happen?
- How much data moved?
- Which protocols and ports were involved?

At a high level:

- Nodes represent endpoints (hosts, devices, PLCs/HMIs, servers, routers, Internet nodes).
- Edges represent communication between endpoints, aggregated into flows with metrics (bytes, packets, protocol/port sets, timestamps).

NDA is optimized for fast post-capture investigation:

1. Ingest one or more PCAPs and immediately see the "shape" of the network.
2. Narrow quickly using filters (time window, protocol/port, OT-only, insecure, Internet/broadcast, query language).
3. Inspect endpoints and flows to understand what happened.
4. Export findings (images/PDF, JSON/CSV, read-only project snapshots) for reporting or collaboration.
5. Save a project (.ndap) to resume later; export Read-Only project snapshots for sharing (Individual/Enterprise).

1.1 Typical use cases

- Incident triage:
  - Identify new external connections and unexpected destinations.
  - Spot scanning behavior (many low-byte edges from one source).
  - See unusual lateral movement (new internal peers, new management ports).
  - Export a shareable artifact for incident notes and reporting.
- OT safety review:
  - Isolate OT protocols and OT-only edges.
  - Confirm insecure services are not present in OT zones.
  - Use Command Center (requires Individual) to summarize inventory and incidents (if present in your build).
- Network change verification:
  - Compare baseline vs after-change states using Graph Diff (requires Individual).
- Reporting and collaboration:
  - Annotate the canvas (shapes, labels, legends, connectors).

  - Export a high-resolution PNG/SVG/PDF via Export Hub.
  - Export a Read-Only project snapshot (.ndap) so others can explore without modifying the workspace (requires Individual).

1.2 Data handling and privacy (practical)

- NDA performs analysis locally. It does not upload your PCAP by default.
- The Desktop build stores your projects and exports locally (paths vary by environment).
- The Web Viewer build uses browser storage (OPFS) when available for persistence; if storage is denied or unavailable, persistence may be limited.
- Some optional experiences may open external links (for example Feedback forms). Core investigation works offline.
- Some builds include embedded enrichment data (for example IP geolocation via IPinfo Lite) so Internet nodes can be labeled without network access.

1.3 What NDA is (and is not)

NDA is:

- A fast visual analyzer for PCAP-based investigations.
- A workflow tool (projects, annotations, exports, diffs, and OT dashboards when enabled).

NDA is not:

- A live IDS/IPS (unless your deployment includes capture services feeding it).
- A TLS decryption tool. NDA can parse TLS metadata, but it cannot reconstruct encrypted HTTP bodies without decrypted payloads.

2. Editions, Licensing, and Feature Gates

NDA can run in Free mode or licensed modes (Individual, Enterprise). Features are enabled/disabled by your license plan and, in some environments, by deployment settings.

Two important principles:

- Feature availability can vary by build/deployment. Some buttons may be hidden in a build that does not ship a feature.
- Licensing is evaluated locally. Use Settings -> License as the source of truth for your current plan.

2.1 How to check your current mode

- Look at the plan badge in the top bar (for example Free).
- Open Settings -> License to view:
  - license status and plan (Free/Individual/Enterprise)
  - expiration/metadata (if shown in your build)
  - actions: Install License, Refresh, Remove License

2.2 Common gated capabilities (high level)

Your environment may enable a subset or superset of these. Always treat Settings -> License as the source of truth.

Simplified plan model:

- Free: core non commercial use
- Individual: unlocks advanced workflows and licensed for commercial use
- Enterprise: includes all Individual features (plus any org-specific additions)

Capability	Requires	What it enables
Multi-canvas editing	Individual	Multiple canvases (tabs) per project
Graph Diff	Individual	Compare snapshots/time windows with overlays + export graph_diff.csv
Asset CSV import	Individual	Enrich nodes using your own inventory CSV
Vendor/OUI import	Individual	Import updated vendor/OUI mappings
Read-Only project exports	Individual	Export read-only .ndap snapshots for sharing
Command Center	Individual	OT inventory/ incidents/ insights/ workflows/ playbooks

Additional notes:

- Enterprise includes everything in Individual.
- Some deployments may still hide or disable specific UI surfaces via build or deployment settings even when your license plan is correct.

2.3 Installing or updating a license (step-by-step)

Common entry points:

- The first-launch license dialog (if shown), or
- Settings -> License

Steps:

1. Open Settings -> License.
2. Click Install License.
3. Select the license file provided by your administrator/vendor.
4. Confirm the status badge updates to a licensed state.
5. Confirm the plan label shows the expected plan (Individual or Enterprise) for the capabilities you need.

If features still appear locked:

- Click Refresh (if your environment supports refresh).
- Close and reopen NDA after installing the license.

TIP	If a license appears expired unexpectedly, confirm your system clock is correct.

2.4 Troubleshooting licensing and locked features

If a feature remains locked or missing:

- Confirm your plan is Individual or Enterprise in Settings -> License.
- Some features may require both a license and a build that ships the feature (or a deployment that enables the UI surface).
- If a button is entirely absent (not disabled), your build may not include that capability.

3. Core Concepts (How NDA Thinks)

This section gives you the mental model NDA uses. If you understand these concepts, the UI becomes predictable.

3.1 Capture vs ingest job vs dataset

- Capture file: the raw input (.pcap / .pcapng).
- Ingest job: NDA parsing that file to build a graph.
- Dataset: the in-app representation of a capture. If you load multiple PCAPs, NDA may treat them as multiple datasets and let you toggle visibility.

3.2 Nodes (endpoints)

A node represents an endpoint. A node may have:

- identity: id, name, ip, mac
- classification: type (router, switch, server, PLC, etc.)
- enrichment:
  - vendor/manufacturer (often from MAC OUI)
  - custom metadata (meta.*) from asset CSV import (requires Individual)
  - geo/org enrichment for public IPs (country/ASN/org) when available

3.3 Edges (communication)

An edge represents aggregated communication between two nodes:

- total bytes and packets
- first/last observed timestamps
- observed protocol set (TCP/UDP/ARP/... plus application hints where available)
- observed port set
- flags: insecure/OT/internet/broadcast/encrypted/vlan/... (varies by build)

One edge typically summarizes many underlying packets. Think of an edge as: "everything A and B did with each other in this dataset/time slice."

3.4 Filters vs time window vs playback

- Filters decide what is visible.
- Time window is a filter that restricts data to a time slice.
- Playback is a visualization that animates activity; it does not change the underlying capture.

3.5 Layout, pins, Lock Positions

- Layout controls how nodes are arranged (Force-directed, Circular, etc.).
- Pinning holds selected nodes in place against layout forces.

- Lock Positions prevents accidental moves and may block disruptive operations until you confirm.

3.6 Projects and view-only projects

- A project (.ndap) is a saved workspace containing datasets, canvases, layout state, annotations, and export presets (when enabled).
- A view-only project is a read-only .ndap snapshot designed for sharing. Recipients can open, filter, and export images/data, but cannot modify datasets or export a full editable .ndap.

4. First Launch Checklist

Use this checklist before ingesting real incident/OT data.

4.1 Confirm your mode and license

1. Open Settings -> License.

2. Verify:

- the mode you expect (Free/Individual/Enterprise)
- that your plan is correct for your workflows (Individual/Enterprise for advanced features)

4.2 Set critical preferences (before ingest)

Performance settings (if you expect large graphs)

1. Open Settings -> Performance.

2. Consider enabling:

- Performance Mode
- Max visible edges (Auto or a safe cap)

If performance is inconsistent:

- Try switching the render backend (WebGL <-> Canvas2D) in Settings -> Performance.
- Lower label density in the Layout panel before increasing edge caps.

Visual defaults

1. Open Settings -> Visual.

2. Choose a Node size mode:

- Static (best readability)
- Degree / Bytes / Packets (best for "find top talkers")

3. Enable Show minimap if you expect large graphs.

Optional but recommended:

- Settings -> General:
  - Choose Theme (Dark/Light/Auto)
  - Decide whether to Show grid
  - Enable Auto layout scaling if you frequently change filters on large graphs

Vendor and risk classification tuning (optional)

If you rely heavily on vendor and risk labels:

- Import an updated OUI pack (requires Individual): Settings -> Exports -> Vendors / OUI -> Import OUI

- Review insecure and OT port lists: Settings -> Visual -> Port lists

4.3 Storage planning (projects and exports)

Even in Free mode, NDA creates on-disk artifacts:

- Projects you save (.ndap)
- Exports you generate (PNG/SVG/PDF/JSON/CSV)

Desktop builds commonly store user data under your Documents directory, for example:

- Documents\FlowTrussNDA\...
- On OneDrive-enabled systems this may resolve under OneDrive\Documents\FlowTrussNDA\...

Practical planning guidance:

- Keep free disk space available if you work with large captures or high-resolution exports.
- In managed environments, confirm where projects/exports are written and how they are backed up.

5. Quick Start (5-10 minutes)

1. Open NDA.

2. Load a PCAP:

- Drag and drop a .pcap / .pcapng onto the canvas, or
- Open the Ingest panel and click Open PCAP.

3. Confirm ingest completed:

- top bar counters (Nodes/Edges/Packets/Bytes) update
- the graph appears on the canvas

4. Explore:

- zoom (mouse wheel), pan (drag background)
- click a node -> Inspector shows endpoint detail
- click an edge -> Inspector shows flow detail

5. Filter quickly:

- toggle Hide Internet to focus internal traffic
- toggle OT only (if applicable)
- enter a query like proto:modbus port:502

6. Export a visual:

- open Export Hub (Ctrl/Cmd+Shift+E)
- export a PNG (or PDF) of the current view

7. Save and share:

- Save a project (.ndap) to preserve your work
- Export a Read-Only project (.ndap) to share safely (requires Individual/Enterprise)

6. Interface Tour

This section maps the UI to common tasks. Names below match typical on-screen labels.

If something described here is missing in your build:

- It may be locked by license (see Settings -> License), or
- It may be disabled by a feature flag, or
- It may not ship in your build.

6.1 Top Bar (status and search)

The top bar has two "cards":

Left card:

- Product name and plan badge (for example "Free")
- Live stats chips:
  - Nodes, Edges, Packets, Bytes
  - Time window chip (often "Full capture" until you narrow it)
  - Selected chip (appears when you have an active selection)
  - Diff chip (appears when Graph Diff overlays are active)
- Search row:
  - Search input: enter filter language queries
  - Help button: opens a "Filter Language" example panel

Right card:

- Toolbar buttons (undo/redo, panels, projects, export hub, settings)

TIP	Use Ctrl/Cmd+/ to focus the search input quickly.

6.2 Toolbar (global actions)

Common toolbar actions (left-to-right in many builds):

- Undo / Redo
  - Primarily affects edits such as annotations, groups, and some workspace actions.
- Command Center (requires Individual)
  - Opens an OT workflow surface (inventory/incidents/insights/workflows/playbooks).
- Toggle Panels
  - Shows/hides docked panels (sidebar, inspector, and other dock zones).
  - Shortcut: Ctrl/Cmd+P.
- Save Project

  - Shortcut: Ctrl/Cmd+S (Save) and Ctrl/Cmd+Shift+S (Save As).
- Recent Projects
  - Opens recovered sessions and saved projects.
- Export Hub
  - Shortcut: Ctrl/Cmd+Shift+E.
- Settings
  - Opens the Settings dialog (General/Visual/License/Exports/Performance/Feedback).

6.3 Left Sidebar Panels (Ingest, Layout, Filters)

The left sidebar is scrollable and panels are collapsible.

Ingest panel

Header hint: "Drop files on canvas"

Primary controls:

- PCAP / PCAP-NG
  - Open PCAP: choose one or more .pcap/.pcapng files
  - Demo: loads a demo dataset (useful for learning the UI)
  - After loading multiple files, "Uploaded PCAPs" may appear and let you manage visibility
- Assets (requires Individual)
  - Upload CSV...: import inventory data to enrich nodes
  - CSV format help (help icon): shows required/recommended columns and a sample CSV

Layout panel

Header hint: "Auto-scales to graph size"

Controls and what they do:

- Layout
  - Force-directed: general-purpose discovery layout
  - Block Grid: structured clusters
  - Circular: presentations and small graphs
  - Orthogrid: grid-like layout for readability
  - Ranked L-R: left-to-right structure for directed-looking views
  - Radial by Subnet: groups endpoints by subnet and radiates outward
- Scale: spreads nodes out (higher = more space)
- Edge Width: visual thickness
- Edge Style: switches edge rendering theme

- Labels
  - Density: how many labels are drawn
  - Auto: let NDA adjust label density based on graph size
  - Label Size: font size used for node labels
- Pinning hint: Shift+Click pins/unpins a node

Filters panel (including time and playback)

Header hint: "Zoom selection"

Core filters:

- Internet (drop-down)
  - Both
  - Show Internet only
  - Hide Internet
- Broadcast (drop-down)
  - Both
  - Hide Broadcast
  - Show Broadcast only
- OT only (checkbox): restricts view to OT-tagged edges
- Highlight insecure (checkbox): visually accent insecure edges
- Hide orphaned nodes (checkbox): hides nodes with no visible edges after filtering
- IP Version (drop-down): IPv4 only / IPv6 only / both

Protocol and port filters:

- Protocol: opens a "Select Protocols" dialog
- Ports: freeform port list and ranges (for example 80,443 502-504; 22)
- All required: if checked, an edge must include every port you listed; if unchecked, any match is sufficient

Time and playback:

- Time Window: start/end sliders
- Playback: Play/Pause plus edge animation speed slider
- Reset: resets filter state (a fast recovery button when you hide everything)

6.4 Canvas and Minimap (exploration)

Canvas basics:

- Zoom: mouse wheel / trackpad scroll
- Pan: drag empty canvas
- Select: click a node or edge
- Reposition: drag nodes (unless pinned/locked)

Fit and focus:

- Fit full graph: Ctrl/Cmd+Shift+F
- Center selection: use the Inspector Center button

Minimap:

- Shows a navigation overview ("Minimap - click/drag to pan")
- Can be toggled in Settings -> Visual -> Show minimap

6.5 Canvas Control Rail (quick actions)

The canvas control rail is a compact vertical action strip.

Rail toggle:

- "Hide canvas controls" collapses the rail to reduce clutter.

Common actions:

- Add Annotation (menu)
  - Text Block, Rectangle, Circle, Legend, Connector Line, Image
- Unpin All: removes all node pins
- Lock Positions (toggle): prevents layout changes from moving nodes
- Hidden Nodes (eye icon): opens the Hidden Nodes dialog
- Reset Layout: re-applies layout (may prompt to unpin/unlock first)

6.6 Inspector (Details panel)

The Inspector usually docks at the bottom and opens on selection.

Header buttons:

- Center: centers the camera on the selected node/edge
- Close: closes the inspector

Resizing:

- Drag the resize handle along the top edge of the inspector.
- Double-click the resize handle to return to an automatic height.

What you see depends on selection:

- Node selection: identity, metadata, enrichment, rollups
- Edge selection: flow summary (ports, protocols, bytes, packets, first/last seen)

6.7 Settings (where most configuration lives)

Open via the toolbar (sliders icon).

Tabs and key controls:

General:

- Theme (Dark/Light/Auto)
- Show grid
- Auto layout scaling
- Shortcut reference list
- Reset Custom Node Images
- Reset Saved Settings (clears saved preferences and dock layout)

Visual:

- Show minimap
- Node size mode (Static/Degree/Bytes/Packets)
- Default node visuals per type (color/icon/image)
- Edge colors (Insecure/OT)
- Port lists (insecure ports and OT ports)

License:

- Status badge and details
- Plan (Free/Individual/Enterprise)
- Install / Refresh / Remove license actions

Exports:

- Open Export Hub
- Print Graph
- Export Project (.ndap) and Open Project (.ndap)
- Vendors / OUI: Import OUI and Clear OUI (requires Individual)

Performance:

- Performance Mode
- Max visible edges
- Switch rendering engine (WebGL <-> Canvas2D)

Feedback:

- External links for feedback and bug reports (if present)

6.8 Common dialogs and overlays you will see

Protocol picker ("Select Protocols"):

- Lets you search and select protocol tokens; includes Clear/Cancel/Apply.

Hidden Nodes dialog ("Hidden Nodes"):

- Lets you search hidden nodes by name/IP/MAC and restore selected or all.

Group Selection dialog ("Group Selection"):

- Lets you name a group and choose a group color when grouping selections (Ctrl/Cmd+G).

Icon picker ("Choose Node Icon"):

- Lets you choose a predefined icon or upload a custom icon for a node type; can apply to all nodes of a type.

Ingest overlay ("Importing PCAP..."):

- Shows ingest progress and includes Cancel Ingest.

Layout confirmations:

- "Positions/Pins Block Layout" prompt appears if you try to apply changes while Lock Positions is on or nodes are pinned.
- "Reset Layout" prompt warns that reset will unpin and unlock before applying.
- "Change Visible PCAPs" prompt warns that toggling visible PCAPs can reset layout and affect pins.

Export Hub dialog ("Export Hub"):

- Unified exports surface with Visual/Data/Queue tabs (labels can vary by build).

Command Center panel ("Command Center", requires Individual):

- Full-screen OT workflow surface with tabs.

7. Loading Data (Ingest)

7.1 Supported inputs

Common supported inputs:

- .pcap and .pcapng capture files
- .ndap projects (saved workspaces)
- .csv asset enrichment imports (requires Individual)

What NDA "ingests" (important):

- NDA builds a graph representation (nodes and edges) from packets.

If you are not sure what your build supports, start with:

- Ingest a small PCAP
- Open Settings -> License to confirm your plan

7.2 Import a PCAP (drag & drop / Open PCAP)

Drag & drop

1. Drag one or more PCAP files onto the canvas.
2. NDA begins ingest immediately.

Drag and drop tips:

- You can drop files anywhere on the canvas.
- Dropping multiple PCAPs at once is supported in many builds.

Ingest panel

1. Open the Ingest panel.
2. Click Open PCAP.
3. Select one or more .pcap / .pcapng.

Ingest panel tips:

- The file chooser may also allow selecting .ndap to restore a workspace.
- Use Demo when you want to learn features without using real data.

After ingest

You should see:

- updated counters (Nodes/Edges/Packets/Bytes)
- the graph on the canvas
- the time window chip showing full capture (or earliest/latest timestamps if displayed)

If the canvas looks empty after ingest:

- Use Ctrl/Cmd+Shift+F to fit the full graph.
- Click Filters -> Reset.
- Confirm time window is full capture (start=0%, end=100%).

7.3 Multiple PCAPs and visibility toggles

When multiple PCAPs are loaded, NDA may show an Uploaded PCAPs list.

Key behavior:

- Changing which PCAPs are visible changes the graph.
- NDA may warn that toggling visible PCAPs can reset the layout.

Best practice:

- Turn on Lock Positions before toggling datasets if you care about preserving a hand-arranged layout.

What "visibility toggles" typically affect:

- Which packets are included in the current view
- Which nodes/edges exist at all (topology can change)
- Which edges are eligible for Export Hub data exports (JSON/CSV) and Graph Diff snapshots

WARNING	If you pin nodes and then change visible PCAPs, the underlying topology may change and pinned nodes may appear in unexpected places. Use pins for presentation, not as a guarantee of semantic identity across different datasets.

7.4 Cancel ingest safely

If you loaded the wrong file or need to change a setting before ingest:

1. Click Cancel Ingest during ingest.
2. Adjust settings.
3. Re-ingest the PCAP.

Cancel behavior is build-dependent. If you cancel mid-ingest, assume partial results are not suitable for final analysis.

7.5 Asset CSV import (inventory enrichment)

LICENSE	Required: Individual

Use Ingest -> Assets -> Upload CSV... to enrich nodes with your inventory metadata.

Workflow:

1. Click Upload CSV....
2. If you are unsure of the format, click the CSV format help button (question mark icon) to view requirements and a sample.
3. Upload your CSV and confirm enrichment appears on nodes in the inspector.

Common uses:

- Set friendly names for critical assets (for example "PLC-12")
- Add ownership and location metadata (meta.Owner, meta.Location)
- Add tags/notes for reporting

7.6 Demo dataset (learning mode)

The Demo button is designed for:

- Learning filters, layout controls, exports, and annotations
- Testing performance settings without using sensitive data

If you do not see Demo, your build may not ship with a bundled demo dataset.

8. Time Window and Playback

Time window and playback controls live in the Filters panel.

They solve different problems:

- Time window: "Show me what happened in this time range."
- Playback: "Animate activity so patterns are easier to see."

8.1 Time window sliders (time slicing)

The Time Window control has two sliders:

- Start
- End

What it does:

- Restricts the visible graph to traffic that occurred within the selected range.
- Updates the time window chip in the top bar (often "Full capture" at 0% -> 100%).

How to use it effectively:

1. Start broad (full capture) to understand baseline topology.
2. Narrow to an investigation window (incident time, maintenance window, OT event).
3. Combine with protocol/port and query language filtering for faster, cleaner results.

Practical tips:

- If you accidentally narrow the window too far and the graph disappears, reset to full capture.
- When you want to compare two time slices, use Graph Diff timeline mode (requires Individual):
  - Set the global time window, then assign it to Window A or Window B.

Performance tip:

- On very large captures, time slicing is often the highest-impact performance lever. Narrowing the time window reduces the active edge set and can dramatically improve responsiveness.

8.2 Playback (visual animation)

Playback animates the current view.

Controls:

- Play/Pause button
- Edge animation speed slider

Use playback to:

- Notice bursts and quiet periods
- Spot periodic polling or beacon-like patterns

- Make presentations easier to follow

Important notes:

- Playback is visual; it does not change your underlying data.
- Playback can increase render work on large graphs. If performance suffers, pause playback while you adjust filters and layout.

9. Searching and Filtering

NDA gives you three complementary filtering layers:

1. Quick filters (sidebar)
2. Protocol and port filters (sidebar)
3. Filter query language (top search box)

Use them together:

- Start with quick filters to remove noise (broadcast, Internet).
- Narrow with protocol/port filters.
- Use the query language for precise targeting and repeatable investigations.

9.1 Quick filters (sidebar)

Internet

Filters -> Internet options:

- Both
- Show Internet only
- Hide Internet

This filter is based on how NDA classifies endpoints (commonly public vs private IP).

TIP	If you choose "Show Internet only" on an internal-only capture, you may hide everything. Use Reset to recover quickly.

Broadcast

Filters -> Broadcast options:

- Both
- Hide Broadcast
- Show Broadcast only

Broadcast/multicast/ARP can dominate some captures. Hiding broadcast often clarifies the "real" communications graph.

OT only

OT only restricts the view to OT-tagged edges.

How OT tagging typically works:

- Known OT ports (from the OT port list in Settings -> Visual -> Port lists)
- In some builds, additional protocol heuristics may tag OT traffic beyond simple port matching

Highlight insecure

Highlight insecure visually accents edges that match insecure port heuristics.

Important:

- This typically highlights rather than hides.
- The port list is configurable in Settings -> Visual -> Port lists.

Hide orphaned nodes

Hide orphaned nodes hides nodes with no visible edges after all filters are applied.

Use this when:

- You have aggressive filters and want to remove isolated artifacts.
- You are preparing a clean export.

IP Version

IP Version options:

- IPv4 + IPv6
- IPv4 only
- IPv6 only

9.2 Port filters (sidebar)

The Ports input accepts:

- Single ports: 80
- Lists: 80,443,502
- Ranges: 502-504

Separators:

- Commas, spaces, and semicolons are commonly accepted separators.

All required:

- Unchecked: an edge matches if it contains any listed port.
- Checked: an edge must contain every listed port in its port set.

Practical examples:

- Show Modbus/TCP: 502
- Show common web: 80,443
- Show OT range: 20000-20010

9.3 Protocol picker (sidebar)

The Protocol control opens a dialog where you can select one or more protocols.

Workflow:

1. Click Filters -> Protocol -> Any.
2. Type in the filter box to find protocols.
3. Check the protocols you want.
4. Click Apply.
5. Use Clear to remove protocol filtering.

Use this to:

- Focus on OT protocols (for example Modbus, DNP3)
- Exclude noisy protocols
- Isolate suspicious protocol families

9.4 Filter language (search box) - complete reference

The search box supports a structured query language with:

- Fields (for example ip, proto, bytes, meta.Owner)
- Boolean operators (AND, OR, NOT)
- Parentheses for grouping
- Comparators (:, =, !=, >, <, >=, <=, IN)
- Quoted strings (single or double quotes)
- Numeric suffixes (k, m, g, t, p)
- Subnet/range matching for IPs

9.4.1 Matching semantics (how to think about it)

There are two important term styles:

Bare terms (no field):

- Example: siemens
- Behavior: case-insensitive substring search across common node strings (name, IP, MAC, vendor, and some metadata).

Field terms:

- Example: vendor:siemens
- Behavior: case-insensitive field comparison against a specific field.

Comparator basics:

- : and = behave like equals for most fields.
- != excludes matches.
- Numeric fields support >, <, >=, <= (for example bytes>50m).
- IN is most commonly used for IP subnet/range matching (for example ip in 192.168.0.0/24).

Boolean logic:

- AND is implicit: a b c means a AND b AND c.
- OR must be explicit.
- NOT negates the next expression.
- Parentheses control grouping: (a OR b) AND c.

9.4.2 Examples (copy/paste)

```
proto:modbus port:502
ip in 192.168.0.0/24 AND NOT flag:insecure
(type:plc OR type:hmi) AND vendor:siemens
bytes>50m AND duration>10
meta.Owner:"Network Ops" AND country:US
```

9.4.3 Field list (what you can query)

Node-focused fields (and common aliases):

- id
- name (aliases: asset, label, host, hostname, node)
- ip (aliases: addr, address, ipaddr, subnet, net, network, cidr)
- mac
- type (aliases: role, kind)
- vendor (aliases: manuf, manufacturer, oui)
- Geo/org enrichment (when present):
  - country
  - country_code (aliases: cc)
  - city
  - region (alias: state)
  - org (alias: isp)
  - asn
  - timezone (alias: tz)
  - geo (alias: location)
- Metadata:
  - meta.<key> (also metadata.<key>, tag.<key>, note.<key>, comment.<key>)
  - meta alone can target many metadata values

Edge-focused fields:

- proto (edge protocol set)
- port (edge port set)
- bytes (numeric)
- packets (numeric)
- duration (numeric, seconds)

- flag (edge flags)

9.4.4 Subnets and ranges (IP matching)

When you use ip in ..., NDA supports:

- CIDR: 192.168.0.0/24
- Wildcard: 10.1.*
- Range (last octet): 10.1.1.50-100
- Range (full IPs): 10.1.1.10 - 10.1.1.20

9.4.5 Numeric suffixes

Numeric fields accept suffix multipliers:

- k = 1,000
- m = 1,000,000
- g = 1,000,000,000
- t = 1,000,000,000,000
- p = 1,000,000,000,000,000

Examples:

```
bytes>1m
packets>=500
duration>30
```

9.4.6 Literal mode (`-l` / `-literal`)

Literal mode forces strict matching and disables some smart parsing.

Syntax:

- Append -l or -literal to the field name (before the comparator).

Examples:

```
country-l:US
meta.Owner-l:"Network Ops"
```

9.4.7 Null checks (missing values)

Some fields may be missing (for example an endpoint might not have a vendor).

Use null to query missing values:

```
vendor:null
vendor!=null
```

9.4.8 Edge flags (`flag:`)

Flags vary by build and enabled features, but commonly include:

- insecure
- ot

Examples:

```
flag:ot AND NOT flag:insecure
flag:insecure
```

10. Working with the Graph

10.1 Navigate and select

- Zoom: mouse wheel / trackpad scroll
- Pan: drag empty canvas
- Fit the full graph: Ctrl/Cmd+Shift+F

Selection basics:

- Select a node: click a node -> inspector shows endpoint details
- Select an edge: click an edge -> inspector shows flow details
- Clear selection: Escape

Multi-select and lasso (common patterns):

- Lasso select: click-drag on empty canvas to draw a selection box (behavior varies by build).
- Move a selection: hold Ctrl during a lasso drag to move selected nodes.
- Pin a selection: hold Ctrl+Shift during a lasso drag to pin nodes inside the selection.

Grouping selections:

- Group: Ctrl/Cmd+G opens the Group Selection dialog so you can name the group and choose a color.
- Ungroup: Ctrl/Cmd+Shift+G.

Copy/paste:

- Copy selection: Ctrl/Cmd+C
- Paste: Ctrl/Cmd+V

Right-click context menu:

- NDA provides a canvas context menu for selection and annotation workflows.
- Contents are build-dependent, but commonly include actions like add annotation, hide items, group, or icon changes.

10.2 Pinning, Lock Positions, and Reset Layout

Pinning and Lock Positions are protection mechanisms for your layout.

Pin/unpin:

- Pin a node: Shift+Click on the node.
- Unpin all nodes: use the Unpin All button in the canvas control rail.

Lock Positions:

- Toggle Lock Positions in the canvas control rail.
- When on, NDA avoids moving nodes during layout changes and may block operations that would reposition nodes.

Reset Layout:

- Reset Layout re-applies the selected layout algorithm to the current graph.
- If Lock Positions is enabled or nodes are pinned, NDA may show a confirmation dialog ("Positions/Pins Block Layout" or "Reset Layout") to unpin/unlock before continuing.

Best practice:

- Turn on Lock Positions before:
  - Toggling visible PCAPs (datasets)
  - Running layout-heavy operations
  - Preparing a report export
- Pin only the nodes you want to keep as anchors (key servers, PLCs, gateways).

10.3 Hidden nodes

Hidden nodes are a decluttering tool:

- hidden nodes are excluded from view (and most visual exports)
- the underlying data is not deleted

How to use hidden nodes effectively:

- Hide nodes to simplify a view without losing the underlying dataset.
- Use hidden nodes when you want to isolate a cluster or remove known "background" assets.

Restore hidden nodes:

1. Click the Hidden Nodes (eye) button in the canvas control rail.
2. Search hidden nodes by name/IP/MAC.
3. Select nodes to restore and click Show Selected, or click Show All.

10.4 Layout controls (left sidebar)

Layout controls focus on readability and do not change your underlying data.

Layout mode:

- Force-directed: best general-purpose view
- Block Grid / Orthogrid: structured layouts for dense graphs
- Circular: presentations and small graphs
- Ranked L-R: left-to-right structure
- Radial by Subnet: emphasizes subnet grouping

Scale:

- Increases/decreases spacing between nodes.
- If the graph looks too dense, increase scale.

Edge Width and Edge Style:

- Edge Width controls thickness.
- Edge Style selects a visual theme (for example Classic, Neon Bloom, Heatmap Spectrum, Blueprint).

Labels:

- Label density controls how many labels are drawn.
- Auto density lets NDA adjust labeling as the graph size changes.
- Label size controls font size.

10.5 Visual settings (node size, type styles, edge colors)

Open Settings -> Visual:

- Node size mode: Static / Degree / Bytes / Packets
- Default node visuals per type (color/icon)
- Edge colors for insecure/OT
- Port lists that define insecure/OT classification

Node size mode guidance:

- Static: best for consistent readability in reports.
- Degree: helps find "central" nodes (many peers).
- Bytes/Packets: helps find top talkers.

Type styles and icons:

- Use "Default node visuals" to set a color or icon per node type.
- The icon picker supports applying an icon to all nodes of a type and uploading custom icons (build-dependent).

10.6 Annotations (text, shapes, legend, connectors, images)

Annotations turn analysis into a shareable narrative.

Create an annotation:

1. Open the canvas control rail.

2. Click Add Annotation.

3. Choose a type:

- Text Block (notes and labels)
- Rectangle / Circle (highlight clusters)
- Legend (explain styling and types)
- Connector Line (link nodes or callouts)
- Image (drop in diagrams or external legends)

4. Place it on the canvas (click or click-drag depending on type).

Edit annotations:

- Select: click the annotation.
- Move: drag it.
- Delete: select it and press Delete.
- Copy/paste: Ctrl/Cmd+C and Ctrl/Cmd+V.

Report tip:

- Use rectangles/circles to isolate areas, then add a Text Block explaining why the region matters (ports, protocols, risk).

Use the Add Annotation menu:

- Text Block, Rectangle, Circle, Legend, Connector Line, Image

Annotations can be included in exports (visual exports and JSON/NDAP when enabled).

11. Inspector (Nodes and Flows)

The Inspector is your drill-down tool for whatever is selected on the canvas. It is the fastest way to move from "shape of the graph" to "what does this endpoint/flow represent?"

11.1 Node inspector (endpoints)

Use the node inspector when you want to understand a single endpoint.

Common fields you will see:

- Identity: name, IP, MAC, vendor
- Type/classification (build-dependent): router, switch, server, PLC/HMI, etc.
- Enrichment: public IP geo/org labels (when available), OUI vendor labels, and any imported meta.* fields
- Connectivity: peers, top ports, protocols, and rollups (build-dependent)

Practical workflow:

1. Click a node on the canvas.
2. Confirm identity (IP/MAC/vendor) and type.
3. Use peers/top ports to understand what it talks to and how.
4. Apply filters (query, protocol, port, time window) to isolate a smaller neighborhood around the node.

11.2 Edge inspector (flows)

Use the edge inspector when you want to understand a single conversation between two endpoints.

Common fields you will see:

- Endpoints (A and B) and direction hints
- Bytes/packets and first/last seen timestamps
- Protocol and port sets (for example TCP/UDP plus ports 80/443/502)
- Flags (build-dependent): insecure, OT, broadcast/Internet, etc.

Practical workflow:

1. Click an edge on the canvas.
2. Confirm which endpoint initiated the flow (when shown) and the ports/protocols involved.
3. Narrow with filters (time window + protocol/port + query language) until the edge represents the traffic you care about.

11.3 Inspector tips (speed and accuracy)

- Center on selection: use the Inspector's Center button (or the equivalent shortcut/button in your build) to keep the selection in view.

- Pair with filters: the Inspector tells you what a selection is; filters let you quickly answer "show me more like this".
- Expect build variance: some builds surface additional rollups or panels, but the node/edge mental model stays the same.

12. Projects (`.ndap`), Autosave, and Sharing

12.1 What a project contains

- Datasets and their visibility state (which PCAPs are included in the current view)
- Canvases/tabs (multi-canvas requires Individual)
- Filters and query text
- Time window and playback settings
- Layout configuration (layout type, scale, label density, edge style)
- Pins, Lock Positions, and camera position (what you were looking at)
- Hidden nodes state
- Groups and annotations (text, shapes, connectors, images)
- Enrichment state (asset CSV import results, OUI pack, type styles, custom node icons)
- Export Hub presets and recent jobs (many builds)

Think of a project as "the investigation workspace", not just the raw capture file.

12.2 Save, Save As, Export Project, Open Project

The most reliable entry points are the UI buttons:

- Toolbar: Save Project (disk icon)
- Toolbar: Recent Projects (history icon)
- Settings -> Exports: Export Project (.ndap) and Open Project (.ndap)

Common shortcuts (as shown in the UI tooltip):

- Save: Ctrl/Cmd+S
- Save As: Ctrl/Cmd+Shift+S

NOTE	Shortcut mappings can vary by build. If a shortcut does not work, use the toolbar and Settings entry points.

12.3 Recent Projects and recovery

Recent Projects is your recovery and fast-open surface.

Typical uses:

- Restore an autosaved session after an unexpected close
- Reopen a saved investigation
- Start a new workspace

If your build shows a "Recent Projects" dialog on startup, it is offering to restore an autosaved project.

12.4 View-only projects (read-only `.ndap`)

License required (to export Read-Only projects): Individual

View-only exports are designed for safe sharing.

Recipients can typically:

- Open and explore the graph
- Change filters and time window
- Export images and data (depending on their build)

Recipients cannot typically:

- Add or remove PCAPs (datasets)
- Modify the project and re-save it as an editable .ndap
- Export a new .ndap project

12.5 Multi-canvas workflow

LICENSE	Required: Individual

Multi-canvas lets you keep multiple investigative views in one project.

UI behavior:

- A row of canvas tabs appears (with left/right arrows and a + button).
- Right-click a tab to Rename, Duplicate, or Delete.

Recommended workflow:

- Canvas 1: baseline topology (full capture, minimal filters)
- Canvas 2: OT-only view (OT filters and port/protocol focus)
- Canvas 3: incident window (narrow time slice plus query)
- Canvas 4: report-ready export (locked positions and annotations)

Export interactions:

- Export Hub can target the current tab, all tabs, or a custom tab list depending on export type.

13. Export Hub (Visual and Data)

Export Hub consolidates exports into a single dialog with presets, advanced visual controls, and a unified queue.

13.1 Open and understand Export Hub

Open Export Hub via:

- Toolbar Export Hub button
- Shortcut Ctrl/Cmd+Shift+E
- Settings -> Exports -> Open Export Hub (when present)

Export Hub is organized into tabs:

- Visual
- Data
- Queue (job history and progress)

The footer includes:

- View docs (opens local docs when available)
- Status messages
- Cancel and Run export buttons

13.2 Presets (repeatable exports)

Presets let you standardize export settings for your team:

- Output format and sizing
- Tiling strategy
- Layer ordering and visibility
- Data scopes and anonymization toggles

Common workflow:

1. Configure settings for a desired output (for example "Poster PDF").
2. Save a preset from the preset menu (three-dots menu next to the preset selector).
3. Reuse the preset for future exports.

Preset menu actions commonly include:

- Save preset
- Reset to defaults
- Delete preset

13.3 Visual exports (PNG / SVG / PDF) - detailed workflow

Use Visual exports for report-ready images.

13.3.1 Visual preview (if enabled)

Some builds include a Visual preview pane:

- "Visual preview" renders a live capture preview before exporting.
- Preview controls typically include zoom in/out and reset.
- Preview may lower quality automatically on constrained GPUs to stay responsive.

If preview is disabled:

- Export still works; you simply do not get the live preview pane.

13.3.2 Sizing, scale, bounds, and background

Typical sizing controls:

- Resolution presets (for example 1080p, 4K UHD, Poster, Square)
- Width (px) and Height (px)
- Lock aspect ratio
- Resolution and/or scale controls (build-dependent)
- Background:
  - Match theme
  - Light
  - Dark
  - Transparent

Fit bounds:

- Enable Fit current view bounds when you want to export only what is currently visible.
- Adjust padding to avoid clipping labels and annotations.

Tile download:

- Individual files (each tile as a separate file)
- Single zip (recommended for many tiles)

13.3.3 PDF layout (PDF exports only)

Common PDF controls:

- Page preset (Letter/Legal/Tabloid/A4/A3)
- Orientation (Portrait/Landscape)
- Page resolution
- Margin
- Renderer mode (bitmap JPEG vs vector SVG, depending on build)

Practical guidance:

- Use higher resolution for print-quality PDFs.
- Use vector mode when you need crisp text and scalable edges (if supported).
- Use bitmap mode when you need maximum compatibility.

13.3.4 Layout refinement (export-time readability)

Layout refinement applies temporary tweaks for export quality without permanently changing your workspace.

Common controls:

- Layout scale (temporary)
- Label density and label size (temporary)
- Freeze selection/highlights (prevents selection glow from being captured)
- Label leader lines and pills (improves label readability for dense clusters)
- Run label-safe reflow (attempts to reduce label overlap)
- Generate layout snapshot (captures an export-time layout snapshot, runs export, then restores your view)

Best practice:

- Use layout refinement when your on-screen view is optimized for exploration, but you need a cleaner exported artifact.

13.3.5 Tiling and multi-page (large graphs)

Tiling is how you export huge graphs without losing resolution.

Modes:

- Rows and columns (manual grid)
- Auto by edges (automatic tiling to stay under edge budgets)

Manual grid controls:

- Rows / Columns
- Padding (px)
- Tile overlap (%)

Auto controls:

- Max edges per tile
- Minimum tile count
- Maximum tile count

Metadata and output options:

- Append tile coordinates to filenames (helps keep tiles organized)
- Embed tile metadata (SVG/PDF)
- Stitch tiles into a single file (when supported)

13.3.6 Layering and visibility

Layering controls let you:

- Reorder draw layers (grid/edges/nodes/labels/annotations)

- Toggle visibility for each layer during export

Common toggles:

- Show background grid
- Show annotations
- Show label flags
- Show diff overlays (when Graph Diff is active)
- Show minimap highlight
- Label clipping backgrounds

13.3.7 Running a visual export

1. Configure sizing/background and (optionally) fit bounds.
2. Configure PDF layout (PDF only).
3. Configure layout refinement and/or tiling for readability.
4. Review summaries in each section.
5. Click Run export.
6. Use the Queue tab to monitor progress.

13.4 Data exports - detailed workflow

Use Data exports for structured outputs and collaboration artifacts.

13.4.1 JSON and NDAP

JSON scope options commonly include:

- All canvases
- Visible subset

Common JSON options:

- Only include selected nodes/edges
- Include annotations
- Hash IP addresses
- Hash MAC addresses
- Strip metadata payloads

Use cases:

- JSON: integrate with scripts, SIEM enrichment, offline analysis, or custom pipelines.
- NDAP: export a project snapshot (editable workspace) for yourself or trusted collaborators.

WARNING	Anonymization is destructive in the exported artifact. Keep an unmodified project for internal use if you may need original identifiers later.

13.4.2 CSV suites (Flow CSV and Inventory CSV)

Flow CSV typically includes:

- Edge-level metrics (bytes, packets, duration)
- Protocol and port sets
- Derived stats (build-dependent)

Common Flow CSV options:

- Scope: All data / Visible / Selection
- Protocol filter (for example tcp,udp,modbus)
- Port filter (for example 80,502)
- OT flows only
- Column selection (select all / select none)

Inventory CSV typically includes:

- Node identity (name/IP/MAC/vendor/type)
- Traffic rollups and peer counts
- Optional embedded images (build-dependent)

Common Inventory CSV options:

- Scope: All data / Visible / Selection
- Type filter and/or OT-only toggles (build-dependent)
- Column selection (select all / select none)

13.4.3 Read-Only project export (read-only `.ndap`)

LICENSE	Required: Individual

Common controls:

- Data scope:
  - Current view
  - All data
- Canvas scope:
  - Current tab
  - All tabs
  - Custom (pick specific canvases)
- Include annotations

Use view-only export when:

- You want to share findings without sharing the original PCAP.

- You want recipients to explore safely without modifying the investigation.

13.5 Queue and job history

The Queue tab shows:

- Export jobs launched from Export Hub
- Status updates and completion messages
- In some builds, retry options for partial tile failures

Queue best practices:

- For very large exports, keep the Queue tab open to watch progress.
- If you export many tiles, prefer "Single zip" to simplify handling.

14. Graph Diff (Compare Datasets/Views)

Graph Diff lets you compare two states of the graph and highlight:

- Additions (new nodes/edges)
- Removals (missing nodes/edges)
- Changes (same items, different metrics)

LICENSE	Required: Individual

If locked, the Graph Diff panel will show "Graph Diff Locked" with a button to manage licensing.

14.1 Where Graph Diff lives

Graph Diff appears as a collapsible panel in the left sidebar called Graph Diff.

It includes:

- Mode: Off / Snapshots / Timeline
- Summary counters: Add / Remove / Change
- Snapshot A and Snapshot B capture controls (Snapshots mode)
- Window A and Window B assignment controls (Timeline mode)
- Threshold controls ("Changed if" bytes or fraction)
- Overlay visibility toggles
- Actions: Apply, Clear all, Export CSV

Top bar:

- When diff is active, a Diff chip may appear showing + / - / ? counts.

Shortcut:

- Press D to toggle diff on/off (when not typing in an input field).

14.2 Modes and what they mean

Mode: Off

- Diff overlays are disabled.

Mode: Snapshots

- Capture Snapshot A and Snapshot B from the current view and compare them.
- Best for before/after comparisons (filters, dataset visibility, investigation stages).

Mode: Timeline

- Assign two time windows (Window A and Window B) using the global time window sliders.
- Best for comparing two time slices within a single capture.

14.3 Snapshots mode (A/B) - step-by-step

Use Snapshots mode to compare different filter states, dataset visibility, or investigation stages.

1. Prepare Snapshot A (baseline):

- Set filters/query/time window to represent the baseline.
- Set Mode to Snapshots.
- Click Capture from current view under Snapshot A.

2. Prepare Snapshot B (comparison):

- Change something (filters, query, time window, visible PCAPs, protocol selection).
- Click Capture from current view under Snapshot B.

3. Optional snapshot controls:

- Swap A/B swaps baseline and compare.
- Focus changes (when enabled) zooms to changed regions.

4. Choose thresholds ("Changed if"):

- Bytes: absolute delta threshold (for example 1,000,000 bytes)
- Fraction: fractional delta threshold (for example 0.20 = 20%)
- An item is considered "changed" if it meets either threshold.

5. Choose compare behavior:

- Treat edges as undirected helps when direction may swap.

6. Choose what overlays to show:

- Additions / Removals / Changes
- Only changed items hides additions/removals and focuses on deltas.

7. Click Apply to compute and render overlays.

8. Investigate:

- Click an overlaid node/edge and use the inspector.
- Many builds add a "Diff (A vs B)" card to the inspector with before/after metrics.

9. Export:

- Click Export CSV to download graph_diff.csv.

14.4 Timeline mode - step-by-step

Use Timeline mode to compare two time slices from the same capture.

1. Set Mode to Timeline.

2. Use the global time window sliders (Filters panel) to select a time slice.

3. Click Use current time window under Window A.

4. Move the global time window to another slice.

5. Click Use current time window under Window B.

6. Adjust thresholds and overlay toggles as needed.

7. Click Apply.

Convenience controls:

- Split capture 50/50 sets A and B to the first and second halves of the capture.
- Swap windows swaps Window A and Window B.

14.5 Practical interpretation tips

- Use the time window chip in the top bar to confirm you are comparing the intended ranges.
- Start with higher thresholds (reduce noise), then lower thresholds when you are confident the baseline is correct.
- Use Only changed items when additions/removals are too noisy.

15. Command Center (OT Workflows)

Command Center consolidates OT-focused workflows into a single surface.

LICENSE	Required: Individual

If disabled or locked, the toolbar button may be hidden or will open a license prompt.

15.1 Open Command Center

1. Use the toolbar Command Center button (if present).
2. Command Center opens as a full-screen panel with tabs:
   - Inventory
   - Incidents
   - OT Insights
   - Workflows
   - Playbooks
   - Timeline and Diff

The header includes:

- A refresh status indicator (for example "Waiting for data...")
- A Close button

If your capture is still processing, tabs may show "loading..." messages until background analysis completes.

15.2 Inventory tab (what to expect)

Inventory typically summarizes:

- Assets (nodes) with identity (name/IP/MAC) and role/type
- Peer count and traffic totals
- Protocol and port summaries
- Risk flags (for example insecure exposure)

Many builds include an Export table action to export the inventory view for offline review.

15.3 Incidents and OT Insights (what to expect)

These tabs are deployment-dependent, but commonly include:

- OT protocol activity summaries
- Hazard or risk indicators
- Counts by protocol or severity

Use them as a starting point, then pivot back to the graph for deep investigation.

15.4 Workflows tab (saved searches and alerts)

Workflows commonly include:

- Save Current Filters (creates a saved search from your current view)
- New Alert (creates a local alert rule)
- Re-evaluate (refresh results)

Saved searches are useful for:

- Repeatable investigations ("show OT-only + insecure")
- Team workflows ("show Internet-only during incident window")

If your environment supports alerts:

- Alerts evaluate saved searches locally and help you flag recurring conditions across captures.

15.5 Playbooks tab

Playbooks are step-by-step guides embedded in NDA. They help standardize responses such as:

- Contain OT command storms
- Reduce insecure protocol exposure
- Review capture drift using diff tools

Use playbooks as checklists when you need repeatable, auditable analysis steps.

15.6 Timeline and Diff tab

This tab summarizes:

- Current time window (absolute and relative)
- Playback status and speed
- Current diff mode (OFF / Snapshots / Timeline)

Actions commonly include:

- Play/Pause
- Reset Window (sets the time window back to full capture)
- Open Diff Controls (scrolls to the Graph Diff panel and closes Command Center)

16. Enrichment and Classification

16.1 Vendor/OUI import

Vendor enrichment maps MAC address prefixes (OUI) to manufacturers. This improves labeling and classification.

LICENSE	Required: Individual

Open:

- Settings -> Exports -> Vendors / OUI

Import workflow:

1. Click Import OUI.
2. Select an OUI pack (CSV or JSON). Many teams use the IEEE oui.csv file.
3. Review the imported prefixes in the summary panel.
4. Use Clear OUI to remove the custom pack and revert to built-in mappings.

Practical notes:

- Importing an OUI pack is a safe, offline operation.
- A custom OUI pack typically persists across reloads for the current user profile.

16.2 Asset CSV import

Asset CSV import enriches nodes with your own inventory data.

LICENSE	Required: Individual

Open:

- Ingest -> Assets -> Upload CSV...

Use the CSV format help button (question mark icon) to see a format reference and a sample.

Format rules (high level):

- Required:
  - Identifier
  - IdentifierType (ip or mac)
- Recommended:
  - Name (display name)
  - ComponentType (role/type classification)
  - IP and/or MAC (additional identifiers)

- Optional:
  - Tags, Notes, Latitude, Longitude
  - Any meta.* columns (for example meta.Owner, meta.Location, meta.SerialNumber)

Matching behavior (typical):

- NDA matches rows to nodes by IP and/or MAC depending on your IdentifierType.
- Some builds accept multiple identifiers in a single cell (comma/semicolon separated) for convenience.
- meta.* columns become searchable metadata fields (for example meta.Owner:"OT Engineering").

16.3 Geolocation and organization enrichment

Some builds enrich public IPs with country/ASN/org data (for example IPinfo Lite). This helps you understand where Internet endpoints likely reside.

Common enriched fields (when present):

- country and country_code
- city and region
- org and asn
- timezone and geo (location)

Important limitations:

- Private RFC1918 IPs do not have public geolocation.
- Geolocation is best-effort and may be coarse.
- Offline environments can still benefit if the enrichment database is embedded in the build.

17. Performance and Scaling

Large captures can produce large graphs. Use the tools below to stay responsive without losing investigative value.

17.1 First-line performance controls (fast wins)

When performance is poor, start here:

1. Remove common noise:

- Broadcast -> Hide Broadcast
- Internet -> Hide Internet (if you only care about internal traffic)

2. Narrow scope:

- Filter by protocol and/or ports
- Use the query language to focus on a subset

3. Time slice:

- Narrow the Time Window to a smaller range

17.2 Performance Mode and edge caps

Open Settings -> Performance:

- Performance Mode (speed): reduces visual complexity and may change sampling strategy (build-dependent).
- Max visible edges: cap the number of edges rendered. Use Auto first, then set a cap if the view is still slow.

Practical guidance:

- If the graph "stutters" when panning/zooming, lower label density and cap edges first.
- If the graph is responsive until you hit Play, pause playback while you adjust the view.

17.3 Render backend switching (WebGL vs Canvas2D)

Some builds support switching render backends:

- WebGL: often fastest for large graphs on systems with good GPU acceleration.
- Canvas2D: can be more stable on systems with driver issues or limited GPU resources.

If your graph is slow or unstable:

1. Open Settings -> Performance.

2. Switch the render backend.

3. Re-test basic interactions (pan/zoom, selection, playback).

17.4 Layout and labeling strategies for big graphs

Layout:

- Force-directed is the best starting point but can be busy for huge graphs.
- Try Block Grid or Orthogrid to improve readability on dense captures.
- Increase layout scale to reduce overlap.

Labels:

- Lower label density to reduce clutter and draw cost.
- Reduce label size on large canvases.
- Consider enabling label auto-density so NDA adapts as the graph grows.

17.5 Exporting large graphs without losing resolution

Use Export Hub tiling:

- Export at high resolution (for example Poster)
- Enable tiling (grid or auto)
- Download tiles as a zip for easier handling

This is the recommended way to produce print-ready exports from large graphs.

18. Troubleshooting

This section focuses on the most common failure modes and the fastest paths to recovery.

18.1 "Nothing is visible" (blank canvas after ingest)

Common causes:

- Filters are too aggressive (Internet-only on internal capture, Broadcast-only, OT-only with no OT traffic).
- Port/protocol filters exclude everything.
- Time window is too narrow.
- The camera is not focused on the graph.

Fast recovery checklist:

1. Click Filters -> Reset.
2. Clear the query in the search box.
3. Set the time window to full capture (start=0%, end=100%).
4. Press Ctrl/Cmd+Shift+F to fit the full graph.

18.2 Query shows an error / results look wrong

Common causes:

- Unsupported field name
- Missing value after a comparator
- Unbalanced parentheses

Fix checklist:

- Click the filter language help button next to the search input.
- Start with a simple query and add terms gradually.
- If you need partial matching, use a bare term (no field) instead of a field term.

18.3 "Positions/Pins Block Layout" or layout changes do nothing

Cause:

- Lock Positions is enabled and/or nodes are pinned.

Fix:

- Use Unpin All and toggle off Lock Positions, or accept the confirmation dialog to "Unpin & Apply".

Best practice:

- Use Lock Positions only when you are ready to preserve a report layout.

18.4 Export Hub preview is blank or disabled

Some builds disable preview behind a feature flag.

Workarounds:

- Export without preview (use presets and tiling).
- Use the Queue tab to confirm export status.

If a visual export fails on very large graphs:

- Reduce label density and enable tiling.
- Switch to "Single zip" for tile download.

18.5 Graph Diff is locked or missing

Fix checklist:

- Open Settings -> License and confirm your plan is Individual or Enterprise.
- If the Graph Diff panel shows "Locked", use the Manage license button to install an Individual/Enterprise license.

18.6 Command Center is locked or missing

Fix checklist:

- Open Settings -> License and confirm your plan is Individual or Enterprise.
- If the Command Center button is hidden, your build may not include the feature.

18.7 Asset CSV import did not apply

Common causes:

- IdentifierType mismatch (ip vs mac)
- Identifiers do not match nodes in the capture
- CSV has missing required columns

Fix checklist:

- Confirm your plan is Individual or Enterprise (Asset CSV import is licensed).
- Use the CSV format help button to confirm required columns.
- Verify your Identifier/IdentifierType values match what the capture actually contains.
- After import, click a node and confirm the expected metadata appears.

18.8 OUI import did not change vendor labels

Common causes:

- The capture has no MAC addresses for those nodes.
- The OUI pack is missing the vendor prefix you expect.

Fix checklist:

- Confirm your plan is Individual or Enterprise (OUI import is licensed).
- Confirm nodes have MAC addresses in the inspector.
- Re-import the OUI pack and check the import summary panel for the prefix.

18.9 Where to find logs (Desktop)

When support requests logs, common locations include:

- %USERPROFILE%\\Documents\\FlowTrussNDA\\logs
- %APPDATA%\\FlowTrussNDA\\logs (fallback in some environments)

If you need a clean reset:

- Settings -> General -> Reset Saved Settings clears dock layout, filters, and saved preferences.

19. Appendix (Shortcuts, examples, glossary)

19.1 Keyboard and mouse shortcuts

Action	Shortcut
Zoom	Mouse wheel / trackpad scroll
Pan	Drag empty canvas
Fit full graph	Ctrl/Cmd+Shift+F
Focus search box	Ctrl/Cmd+/
Clear selection / dismiss dialogs	Escape
Pin/unpin node	Shift+Click
Unpin all	Canvas control rail -> Unpin All
Toggle docked panels	Ctrl/Cmd+P
Group selection	Ctrl/Cmd+G
Ungroup selection	Ctrl/Cmd+Shift+G
Copy selection	Ctrl/Cmd+C
Paste selection	Ctrl/Cmd+V
Delete selected annotations/groups	Delete
Undo	Ctrl/Cmd+Z
Redo	Ctrl/Cmd+Y or Ctrl/Cmd+Shift+Z
Save project	Ctrl/Cmd+S
Save project as	Ctrl/Cmd+Shift+S
Open Export Hub	Ctrl/Cmd+Shift+E
Toggle Graph Diff	D (when not typing)

19.2 Sample filter queries (copy/paste)

```
proto:modbus port:502

ip in 192.168.0.0/24 AND NOT flag:insecure

bytes>1m OR packets>500

type:router OR vendor:siemens

flag:ot AND NOT flag:insecure

meta.Owner:"Network Ops"
```

19.3 Sample asset CSV template

```
Identifier,IdentifierType,Name,ComponentType,IP,MAC,Latitude,Longitude,Tags,Notes,meta.Owner,meta.Location,meta.SerialNumber

10.10.3.42,ip,Core Switch A,Switch,10.10.3.42,,47.6205,-122.3493,"network;core","Primary distribution switch","Network Ops","HQ - DC1","SW-CORE-A-001"

00:50:56:21:8F:AA,mac,HV Node 1,Server,,00:50:56:21:8F:AA,37.7749,-122.4194,"compute;tier1","vSphere host","Platform Team","Colo West Pod 4","HV-ESXI-001"
```

```
PRINTER-17,mac,Front Desk
Printer,Printer,10.20.5.55,70:4F:57:AA:BC:D1,40.7128,-74.0060,printers,"Check
toner monthly","Facilities","HQ Level 1 Reception","PR-778899"
```

19.4 Glossary

- PCAP / PCAP-NG: packet capture file formats.
- Dataset: a loaded capture's graph data inside NDA (one or more datasets can be visible).
- Canvas: a workspace tab containing a view of the graph (multiple canvases require Individual).
- Node: an endpoint in the graph.
- Edge: aggregated communication between two nodes.
- Flow: a logical conversation between endpoints (often represented by an edge).
- OUI: Organizationally Unique Identifier (MAC prefix) used to map vendors.
- OPFS: Origin Private File System (browser persistent storage).
- Project (.ndap): NDA workspace file containing data + settings + annotations.
- View-only project: a read-only .ndap snapshot designed for safe sharing (exporting requires Individual).
- Export Hub: unified export dialog for visual and data exports.
- Graph Diff: compare two snapshots or time windows and highlight deltas (requires Individual).
- Command Center: OT workflow surface for inventory/incidents/insights and timeline controls (requires Individual).