Data Processing Service Data and Digital Assets

Service Name: LinkWare Live

For EU customers, data is hosted in the USA.

Export access is restricted to owners only.

(a) Categories of Data and Digital Assets that can be transferred:

EXPORTABLE DATA	DATA STRUCTURE & FORMAT	DATA PORTABILITY & RESTRICTIONS
Project ID, organization ID, creator ID, name, address, coordinates, phone, contact, description, dates, customer, project number, status, result summaries, parent project ID, child count, timestamps, deletion timestamp	projects.ndjson; one JSON object per line	Parent/sub-project relationships preserved through parent_project_id
Result ID, organization ID, project ID, user ID, TST ID, name, media, test standard, cable type, date, status, lengths, coax flag, reportability, calibration status, test-set hashes, timestamps, deletion timestamp	results.ndjson; ts_hashes is emitted as a JSON array	Links to projects, users, tester files, and test configurations
Test ID, organization ID, project ID, result ID, TST ID, type, date, status, operator, test values, limits, margins, fiber values, test standard, cable type, decoded test_data, timestamps	tests.ndjson; test_data is preserved as nested JSON	Contains the main decoded measurement data and links to its result and source tester file
TST ID, organization ID, project ID, file name, file size, timestamps	tsts.ndjson plus original file in tst/<id>.tst	Original tester file is copied without modification; it can be opened with LinkWare PC
Test-set ID, organization ID, project ID, serial number, media, type, module, cable type, test limit, test type, NVP, plot-data setting, test configuration ID, hash, configuration JSON, timestamps	test_sets.ndjson; obj_json is nested JSON	hash connects the test set to Result.ts_hashes; configuration can be reconstructed
Test-setup ID, organization ID, project ID, description, timestamps	test_setups.ndjson	Links test setups to projects

EXPORTABLE DATA	DATA STRUCTURE & FORMAT	DATA PORTABILITY & RESTRICTIONS
Project/test-setup relationship ID, project ID, test-setup ID, timestamps	project_test_setups.ndjson	Preserves which test setups apply to each project
Label-set ID, organization ID, project ID, serial number, label range, type, count, name, labels, test-setup ID, pass/fail/tested totals, hash, configuration JSON, timestamps, deletion timestamp	label_sets.ndjson; obj_json is nested JSON	Preserves label configuration and its project/test-setup relationship
Label ID, project ID, name, date, calibration status, cable type, label-set ID, media, status, test, test standard, headroom, label-set status, creation timestamp	labels.ndjson	Links labels to projects and label sets; label names can match result names
Equipment ID, organization ID, type, model, serial number, hardware version, last test ID, last test date, first-use date, timestamps	equipment.ndjson	Preserves tester identity and its relationship to tests/configurations
Equipment-test ID, equipment ID, equipment configuration ID, test ID, context, creation timestamp	equipment_tests.ndjson	Preserves which tester and configuration produced a test
Equipment-configuration ID, equipment ID, version, calibration date, creation timestamp	equipment_configs.ndjson	Preserves tester firmware/calibration history
Equipment-location ID, equipment ID, latitude, longitude, accuracy, source, address ID, creation timestamp	equipment_locations.ndjson	Coordinates and accuracy remain directly usable; the referenced address record is not included
Report ID, user ID, organization ID, report type, item count, processing status, start/completion dates, timestamps	reports.ndjson plus retained PDF in reports/<id>.pdf	Report metadata is machine-readable; PDFs are included only while retained
Report/project relationship ID, report ID, project ID, timestamps	report_projects.ndjson	Preserves which projects are covered by a report
Project-user relationship ID, project ID, user ID, organization ID, role ID, creation timestamp	project_users.ndjson	Preserves project-level access assignments; users are resolved through Identity member records

EXPORTABLE DATA	DATA STRUCTURE & FORMAT	DATA PORTABILITY & RESTRICTIONS
Organization ID, name, description, addresses, office locations, status, timestamps, LinkWare Live settings	identity/organization.json	Standard JSON that can be consumed independently
Identity member ID, email, username, name, account status, phone, company details, address, language, time zone, timestamps, assigned organization groups	identity/members.ndjson	Open NDJSON; credentials, tokens, login data, and security fields are excluded
Organization group ID, name, description, status, timestamps	identity/groups.ndjson	Open NDJSON; provides role definitions used by member assignments
User ID, application ID, terms version, acceptance timestamp	identity/tos_acceptances.ndjson	Preserves legally significant acceptance history
Original certification report files	reports/<id>.pdf inside the ZIP	Portable PDF format; older PDFs may be unavailable because storage retention is limited
Export metadata, entity counts, schemas, relationships, excluded fields, missing files, caveats, and export version	manifest.json	Self-describing receipt; enables consumers to validate completeness and reconstruct relationships

Organization owners and admins can request a full export of their organization’s data from the Accounts & Settings page and will receive an email when it’s ready to download.

TST File Handling

The original .tst files are included in the export ZIP under tst/<id>.tst. These files are copied in their original, unmodified format. They are not directly human-readable and require LinkWare PC (LWPC) to access the full tester result data, including frequency sweeps and OTDR traces.

In LinkWare PC, users can import the files using:

File → Import From → Test files (.tst)

After importing the .tst files into LinkWare PC, users can inspect the test results and generate reports in the formats supported by LinkWare PC. The export also contains decoded test data in tests.ndjson for machine-readable processing, while the .tst files preserve the complete original tester data for LWPC-based extraction and reporting.

(b) Categories of Data and Digital Assets that cannot be transferred

Data Not Provided:

System and security and internal operational data: Passwords, password hashes, salts, API keys, authentication tokens, login history, lockout counters, and internal platform or queue data are excluded for security reasons.

LinkWare Live reference data: Product-level cable definitions, test limits, standards, and system role definitions are not exported because they are shared platform reference data rather than organization-owned data.

Unresolved address records: Equipment location coordinates, accuracy, and source are exported, but the related address record is not included.

Frequency sweeps and OTDR traces: These are not exported as separate decoded data files because the complete trace data is retained inside the original .tst files rather than in the database.

The following categories of data are not exportable:

Category 1:

Data of Provider or a third party that are protected by intellectual property rights or constituting trade secrets, or any information held by Fluke that (a) derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Category 2: Any information held by Fluke that could reveal information in Category 1.

Category 3: Other information specific to the internal functioning of the service that is not covered by Categories 1 or 2 but whose export would risk breaching Fluke's trade secrets.

(c) Information on procedures for switching and porting with the use of switching tools: Information on the available procedures for switching and porting to and from the Service, including the available switching and porting methods and formats, and the restrictions and technical limitations known to Provider, is set out in Section 3.1 of the EU Data Act Addendum.

(d) Known risks to continuity in the provision of the functions or services of the Source Provider: None

Notice version: 1.0 **Last updated:** 2026-09-10