MEYLAN TECHNOLOGIES & CONSULTING

MTC Skopos

Data Processing & Architecture Whitepaper

The offline processing model and the absence of customer-data egress to MTC

Subject	The offline processing model and the absence of customer-data egress to MTC
Audience	Information security, data protection, procurement, and audit functions
Applies to	MTC Skopos (current releases)
Last reviewed	June 2026
Classification	Public — may be shared with customers and their advisors

1. Executive summary

MTC Skopos is a desktop application for analysing critical-access and segregation-of-duties (SoD) risks in ERP systems (primarily SAP). It runs entirely on the operator's own machine. All data ingestion, risk analysis, remediation, and reporting are performed locally, and every output is written only to the local file system or network location the operator chooses.

The central assurance of this document is:

> **No customer business data — no user identities, role definitions, permissions, HR attributes, usage statistics, risk findings, or any data read from the customer's ERP system — is ever transmitted to MTC (Meylan TC) or any MTC-controlled infrastructure.**

The application opens network connections in only three well-defined situations, none of which sends customer business data to MTC:

Connection	Destination	Controlled by	Carries your ERP data?
License and version check	MTC license service (licence.mtcskopos.com)	MTC	No — entitlement metadata only
Optional AI assistant	The AI provider you configure (Anthropic, OpenAI, Azure OpenAI, self-hosted)	You	Only if enabled; anonymised by default, sent to your provider, never MTC
Optional live SAP extraction	Your own SAP system	You	Read from your system, stored locally, never forwarded

The single connection that reaches MTC infrastructure is the license service. It exchanges entitlement metadata only: it does not see, and is not given, any analysed data.

2. Processing model

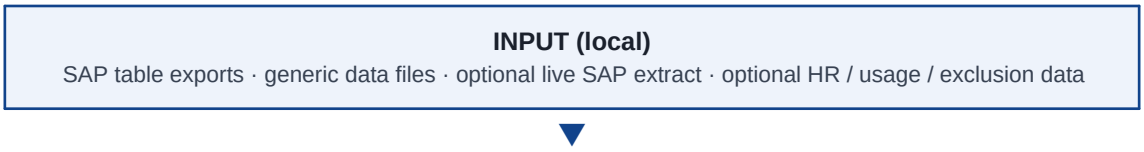
MTC Skopos is a self-contained desktop application. There is no MTC-hosted server component, no cloud tenancy, and no background service that continues after the application is closed.

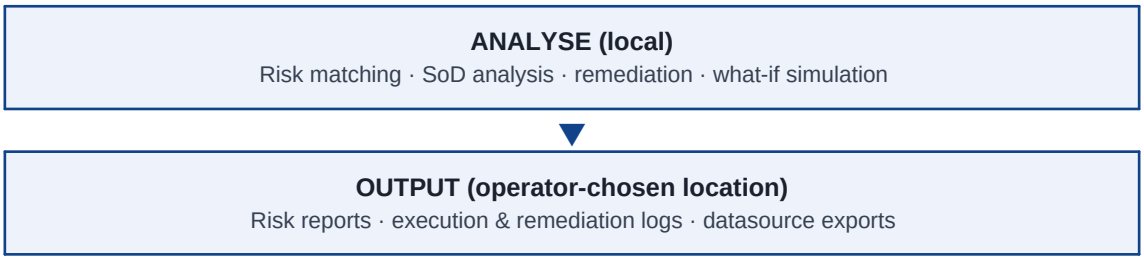
All processing is local. Whatever data the operator loads is read, analysed, and reported on entirely on the operator's machine. There is no external database or remote compute service involved in analysis.

No analysis data is sent anywhere to perform the analysis. Connectivity is not required to analyse data from files; the product operates in restricted-network and air-gapped environments.

3. Data-flow architecture

The end-to-end flow moves from local input to local output and never leaves the operator's machine for the purpose of analysis.





The optional AI assistant is customer-initiated and anonymised by default; it sends data only to an AI provider chosen by the customer, never to an MTC endpoint. The optional live SAP extraction reads directly from the customer's own SAP system; the extracted data is stored locally and analysed against that local copy.

3.1 Input

The operator defines one or more data sources, all referenced locally:

- **Local SAP table exports:** files exported from SAP tables.
- **Generic data files:** exports from non-SAP systems.
- **Live SAP extraction (optional):** a direct connection to the customer's own SAP system to read authorization data. Connection parameters and credentials are supplied by the operator, are used only to reach the customer's system, and credentials are not stored to disk. Extracted data is stored locally and all analysis runs against that local copy.
- **HR, usage, and exclusion data (optional):** additional local files used to enrich and scope the analysis.

Files are selected through the operating system's standard file dialog. There is no upload step.

3.2 Processing

The risk-analysis engine builds its working model locally and performs permission matching and risk detection on the operator's machine. No part of analysis consults a remote service.

3.3 Output

Reports are written to a location the operator selects: detailed and summary risk reports, an execution log that allows the operator to reload a prior analysis offline, remediation reports, and datasource exports. There is no cloud sync or automatic transmission of results.

3.4 Stored settings

Application settings and preferences (selected ruleset, data-source definitions, UI preferences) are stored locally on the operator's machine. No credentials of any kind are stored in these settings. SAP connection credentials and AI provider credentials are held only in memory for the duration of a session and are never written to the stored configuration or to disk. Nothing in this stored configuration is transmitted off the machine.

4. Network connections: complete inventory

The application makes outbound connections in only the three situations below. There is no telemetry, usage analytics, crash/error reporting, or automatic upload of any kind.

4.1 License validation and version check — to MTC, metadata only

- **Destination:** the MTC license service at licence.mtcskopos.com (over HTTPS).
- **What is exchanged:** a signed license entitlement, a machine fingerprint used to enforce seat licensing, periodic heartbeats, and a query for the latest available version — licensing metadata.
- **What is not exchanged:** no personally identifiable information and no business data of any kind (no data-source contents, user identities, roles, permissions, HR data, usage data, or risk findings). The licensing function has no access to analysed data and is never passed any.
- **Frequency:** a check at startup and periodically thereafter.
- **Resilience:** the check fails gracefully. If the license service is unreachable, the application continues to operate against its locally held license within the applicable grace period (approximately three days after the last successful check). This makes restricted-network and air-gapped use practical.
- **Transport security:** HTTPS with certificate verification.

Network allow-listing. The only MTC destination that needs to be reachable is licence.mtcskopos.com over HTTPS (TCP 443). The product remains usable within its grace period if this destination is blocked.

4.2 AI assistant — to the customer's own provider, never to MTC

When the optional AI assistant is used, requests go only to the AI provider the customer configures: the customer's own Anthropic account, an OpenAI-compatible endpoint the customer supplies (including self-hosted and third-party gateways), or Azure OpenAI with customer-supplied details. There is no MTC default endpoint and no MTC fallback for AI. Section 5 details the anonymisation and opt-in controls.

4.3 Live SAP extraction — to the customer's own SAP system

The optional live-extraction path connects directly to the customer's SAP system using operator-supplied parameters. It is a direct connection between the operator's machine and the customer's SAP host; extracted data is stored locally. MTC is not in this path.

4.4 What is demonstrably absent

The product contains no telemetry, usage analytics, or product-metrics reporting; no crash or error reporting to any remote service; no automatic download or installation of updates (only the version-availability check in 4.1; the operator obtains releases through their normal channel); and no MTC data-collection endpoint of any kind.

5. AI assistant: data-protection controls

The AI features are supplementary. The core product (ingestion, risk analysis, remediation, and reporting) is fully functional with AI disabled, including in air-gapped environments.

- **Opt-in and disablement.** AI is gated behind configuration and can be hidden from the interface entirely. With no AI credentials configured, the assistant is simply unavailable. AI credentials are held in memory only and are not written to disk.
- **Bring-your-own-key / bring-your-own-endpoint.** Customers use their own AI account and may direct traffic to a self-hosted or enterprise gateway. MTC never brokers, proxies, or receives this traffic.

- **Anonymisation, on by default.** Before any content is sent to the AI provider, sensitive entities are replaced locally with non-reversible placeholders, and the original values are restored locally on the response. By default this covers user identifiers, single and composite role names, system names, and HR attributes (full name, department, location, user group). The set of anonymised fields is configurable by the operator.
- **Transport security.** All AI requests use HTTPS with certificate verification.

Net effect: even when AI is enabled, the data that leaves the machine goes to the customer's own provider, is anonymised by default, and never reaches MTC.

6. Conclusion

MTC Skopos implements a genuinely offline analysis model. Customer ERP data is read from local files (or pulled directly from the customer's own SAP system), analysed on the operator's machine, and written out only to the location the operator chooses.

The only connection to MTC is the license service, which exchanges entitlement metadata (a license token, a machine fingerprint, and a version query) and never receives analysed data. The optional AI assistant sends data only to the customer's own configured AI provider, anonymised by default, and never to MTC.

> **The product therefore satisfies the requirement it was assessed against: there is no egress of customer business data to MTC.**

7. Appendix: customer-side verification

These checks let a customer confirm the product's behaviour independently, using their own infrastructure and the binary they were shipped, without any access to MTC source code or systems.

7.1 Software integrity and dependency verification

- **Authenticated origin.** The Windows executable is code-signed with a DigiCert-issued Authenticode certificate. A customer can confirm the publisher, and that the binary has not been altered since signing, through the standard Windows signature dialog or with Get-AuthenticodeSignature in PowerShell. A SHA-256 checksum is also published for the distributed archive, giving an independent integrity check over the download channel.
- **Embedded, signature-protected SBOM.** Release binaries are built with cargo auditable, which embeds a complete Software Bill of Materials (every third-party component and its version) inside the executable itself. Because the inventory travels inside the signed binary, its integrity is inherited from the code signature: if the signature verifies, the embedded SBOM is authentic. There is no separate SBOM file whose provenance the customer must take on trust.
- **Independently reproducible scan.** The customer does not need to rely on any scan output supplied by MTC. Running the command below against the signed binary they received extracts the embedded inventory and checks it against the RustSec advisory database, producing the customer's own authoritative result:

```
cargo audit bin mtc-skopos.exe
```

Dependency advisory status. Running the scan against a release may report informational transitive advisories. Each is assessed; in every assessed case none has presented an exploitable condition in Skopos's usage, none enables data egress or remote code execution, and none affects the offline

processing model described in this document. Findings are tracked and addressed through routine maintenance, and the advisory status for a specific release is available on request.

7.2 Behavioural verification checks

- **Network monitoring during analysis.** Run a full file-based analysis with AI disabled and the license service reachable. Capture outbound traffic at the host or firewall. The only MTC destination observed will be licence.mtcskopos.com (HTTPS), exchanging small, periodic licensing requests, not bulk data transfer.
- **Block MTC and confirm continued operation.** Block all outbound traffic except licence.mtcskopos.com, then block that as well. File-based analysis continues to function (within the license grace period of approximately three days), demonstrating that analysis requires no connectivity.
- **Inspect license traffic volume.** Licensing requests are small and infrequent. Their size and cadence are inconsistent with transmission of analysed data sets; this can be confirmed from firewall/proxy logs.
- **AI egress allow-listing.** If AI is enabled, confirm from firewall logs that AI traffic is directed solely to the provider endpoint the customer configured, and to no MTC address. If AI is disabled, confirm that no AI-related egress occurs at all.
- **Output destination review.** Confirm that generated reports appear only at the local or network location the operator selected, with no corresponding outbound transfer to a third party.