

Section III

Publish Workload Requirements Attestation Checklist

We, the vendor, Telmai Inc, confirm and attest to reviewing, meeting, and complying with the requirements outlined in the Microsoft Fabric Extensibility Toolkit specifically the Publish Workload Requirements

The following sections document details, exceptions, or variances regarding the attestation of adherence to the Publish Workload Requirements.

Workload Information

Workload Version	Workload Name	Release Date
1.0.1	Telmai Data Observability	April 2nd

Business Requirements

Value To Customers

The workload must clearly articulate the value proposition and benefits to Fabric customers.

- Supported
- Supported with Notes
- Not Supported

Telmai is a native Microsoft Fabric workload that serves as a data reliability layer, continuously monitoring and validating OneLake data assets. Telmai's ML-driven monitors track volume, schema, freshness, and completeness, generating machine-readable trust signals consumable via MCP by both human users and AI agents, enabling reliable and explainable data-driven decisions.

Trial

We provide an easy and fast trial experience. The trial is available to the customer without waiting time (less than 5 seconds), and provides a free and easy way to explore the offered workload for a limited time in accordance with Microsoft guidelines for Trials

- Yes
- No

Telmai provides a lightweight trial experience that allows Fabric users to install the Telmai workload from the Fabric Workload Gallery and begin monitoring OneLake data products within minutes. The trial enables users to:

- Discover OneLake data products through the Fabric catalog
- Deploy recommended monitors on selected assets
- Run scans, view incidents, and monitoring coverage

The trial provides a limited monitoring scope and feature access and is intended to demonstrate automated monitoring capabilities within Fabric.

Monetization

The workload is available on the marketplace for the customer to procure with or without a trial in accordance with the monetization guidelines

- Yes
- No

Link to the Marketplace Offer:

<https://marketplace.microsoft.com/en-us/product/telmaiinc1760440996162.telmai-fabric-data-observability?tab=Overview>

Technical Requirements

Microsoft Entra Access

The workloads use Microsoft Entra authentication and authorization.

- No other authentication and authorization mechanisms are used
- Different authentication and authorization mechanisms are used for stored data in Fabric
- Telmai authenticates all users exclusively via Microsoft Entra ID JWT tokens
- Workspace RBAC roles (Admin, Member, Contributor, Viewer) are inherited directly from Fabric. No separate identity or credential system is maintained inside Telmai.
- Every request validates three things in sequence:
 - Entra ID JWT
 - Fabric workspace role via the Fabric API
 - tenant registry

One Lake

Workloads integrate with One Lake to store data in the standard formats supported by the Fabric platform so that other services can take advantage of it.

- All data and metadata is stored in One Lake or Fabric Data Stores
- Not all data and metadata is stored in One Lake or Fabric Data Stores

- *Customer data is never moved or replicated outside the customer's Fabric environment.*
- *The Data Plane runs as short-lived Spark container jobs inside the customer's own Fabric account and processes data in place.*
- *Telmai's Control Plane stores only*
 - *Operational metadata (monitor configurations, incident records, and tenant registry) in a Fabric SQL Database*
 - *KQL Eventhouse hosted in Telmai's Azure environment*
 - *Raw data values never leave the customer's Fabric tenant*

Microsoft Entra Conditional Access

Enterprise customers require centralized control and management of the identities and credentials used to access their resources and data and via Microsoft Entra to further secure their environment via conditional access.

- The service works in its entirety with even if customers enable this functionality
- The service works in with limitations if customers enable this functionality
- The service doesn't work Microsoft Entra Conditional Access

Telmai's authentication is entirely Entra ID-based. No alternative auth paths exist. Conditional Access policies enforced at the tenant level apply uniformly to Telmai sessions without degrading functionality.

Admin REST API

Admin REST APIs are an integral part of Fabric admin and governance process. These APIs help Fabric admins in discovering workspaces and items, and enforcing governance such as performing access reviews, etc. Basic functionality is supported as part of the Workload Development Kit and doesn't need any work from Partners.

- Microsoft Fabric Admin APIs are being used (/admin/*)
- No Microsoft Fabric Admin APIs are being used

Customer Facing Monitoring & Diagnostic

Health and telemetry data needs to be stored for a minimum for 30 days including activity ID for customer support purposes, including Trials.

- Minimum 30 days requirement is adhered to
- Vendor stores the data for ___ days beyond the minimum requirement

B2B

The implementation of the workload is in line with Microsoft Fabric's sharing strategy focused on allowing customers to collaborate with their business partners, customers, vendors, subsidiaries, etc. It also means users from other tenants can potentially be granted access to items partners are creating.

- Cross tenant B2B collaboration supported
- Workload Item Access only within the tenant

The Telmai workload inherits Fabric workspace RBAC and identity controls. Each scan runs as an isolated container job scoped to a single tenant. The tenant registry enforces strict tenant boundaries. No data, metadata, or configurations are shared or accessible across tenants. Cross-tenant B2B collaboration is not supported in this release

Business Continuity and disaster recovery

The vendor has a comprehensive Business Continuity and Disaster Recovery (BCDR) plan designed to tackle unplanned disasters and recovery steps.

Telmai maintains a BCDR strategy with nightly database backups, incremental transaction log backups every 30 minutes, and replication to an off-site location, with the last 30 nightly backups retained on a secure transfer server. The platform architecture separates the Control Plane from the Data Plane execution environment to ensure failure isolation — a breach or outage in one does not cascade to the other. BC/DR plans are documented and tested annually. For full terms governing service continuity and data recovery obligations, refer to Telmai's Terms of Service.

Performance

The Workload implementation takes measures to test and track performance of their Items

- Performance Metrics on workload performance are available via the monitoring hub
- Workload includes a separate monitoring UI to test and track performance
- Performance tracking isn't currently available to the end user however vendor support personnel can monitor, test, track performance via their internal instrumentation and monitoring systems

Telmai's Control Plane records all scan execution metrics, anomaly detection results, and pipeline latencies via Azure Event Hub and KQL Eventhouse. This data is available to Telmai engineering and support teams for diagnostics. End-user facing performance dashboards via the Fabric Monitoring Hub are not available in this release.

Presence

To ensure that customer expectations independent of their home or capacity region are met, vendors need to align with fabric regions and clouds. Availability in certain restrictions also impacts your Data Residency commitments.

- Service availability and colocation/alignment in the following fabric regions
- All or part of the service doesn't reside in Azure

Public APIs

Fabric Public APIs are the backbone of automation, enabling seamless communication and integration for both customers and partners within the Fabric ecosystem. Fabric Public API empowers users to build innovative solutions, enhance scalability, and streamline workflows.

- The workload uses Fabric Public APIs

Design / UX Requirements

Common UX

The workload and all item types the partner provides as part of it comply with the Fabric UX guidelines.

- Compliant with Fabric UX guidelines
- The following variance and/or exceptions have been granted by Microsoft

Item Creation Experience

The item creation experience is in accordance with the Fabric UX System.

- Yes
- No

The item creation and onboarding experience follows the Fabric workload installation flow where administrators install the workload from the Fabric Workload Gallery and launch the Telmai interface directly within the workspace.

Monitoring Hub All Long running operations need to integrate with Fabric Monitoring Hub

- Yes
- No

Trial Experience

The workload provides a Trial Experience for users as outlined in the design guidelines

- Trial Supported
- Trial Not Supported

Monetization Experience

The monetization experience is in line with the design guidelines provided

- The monetization experience is integrated with the market place and compliant with the guidelines
- Bring Your Own License (BYOL)
- Free / Freemium
- Other

Telmai offers three monetization options. The Free tier is available via the Fabric Workload Gallery with no payment required, providing a 30-day trial with unlimited monitors followed by an ongoing 50-monitor cap enforced in the backend after 15 days. The Basic tier is a usage-based plan transactable via the Azure Marketplace, metered on active monitor count through Microsoft's commerce system. The Enterprise tier is a private offer with custom pricing, restricted to specific tenant IDs, and negotiated directly with Telmai.

Accessibility

The user experience is in compliance with the Fabric UX design guidelines for Accessibility

- The user experience is compliant with the guidelines
- The following limitations exist

World Readiness / Internationalization

English is supported as the default language. Localization through optional, should be considered.

- English is the only supported language
- The following languages are supported

Item Settings

Item settings are implemented as a part of the ribbon as outlined in the UX guidelines

- Yes
- No

Samples

Samples are optionally provided that preconfigure items of their type to help customers get started more easily.

- Samples not provided
- Samples for preconfiguration of items provided

Custom Actions

Custom actions can be optionally provided as a part of the item editor.

- Custom Actions aren't implemented
- Custom Actions implemented as part of Workload

The following custom actions are implemented within the Telmai workload:

- *Ask Telmai — conversational Copilot for plain-language data quality queries*
- *Deploy Monitors — one-click monitor deployment across selected data products*
- *Schedule — automated scan scheduling based on data update patterns and user-defined intervals*
- *Scan Now — on-demand scan trigger outside the scheduler*
- *Investigate — AI-powered investigation and correlation of incidents across related data products*

Workspace settings

Workspace settings provide a way that workloads can be configured on a workspace level.

- Supported
- Not Supported

Global Search

Searching for items in Fabric is supported through the top search bar.

- Supported

Not Supported

Security / Compliance Requirements

Security general

Protection of customer data and metadata is of paramount importance. Workloads must go through a security review and assessment. Vendor attests that the security review and assessment was completed and will be periodically performed as enhancements and changes are made. Security issues discovered which could have a detrimental impact on the customer should be addressed promptly and customers notified where applicable.

Telmai has completed an independent SOC 2 Type 2 audit covering Security, Availability, and Confidentiality trust service criteria, performed annually by a third party. The report is available to Microsoft and customers under NDA upon request. All data in transit is encrypted via TLS 1.2 and at rest via AES-256. The Fabric workload processes data exclusively within the customer's Fabric tenant using short-lived Spark container jobs — no raw data, PII, or query results are transmitted to or stored in Telmai's infrastructure. Authentication is exclusively via Microsoft Entra ID with JWT token validation on every request, with no alternative auth paths.

Reference: <https://www.telm.ai/product/security-and-compliance/>

Privacy

Partners that build workloads also have a responsibility to protect that data when they access it. Every workload goes through a privacy assessment and a privacy review. Vendor attests that privacy review was completed and is periodically performed as enhancements and changes are made.

****Extra Requirements:**

- Publisher attests that only essential HTTP-only cookies are used by the Workload and only after positively authenticating the user.
- Publisher attests that it's not using or relying on third-party cookies as part of their solution.
- Publisher attests that's obtaining any Microsoft Entra token using the JavaScript APIs provided by the Fabric Workload Client SDK

Telmai performs privacy reviews for its platform architecture and AI features. The platform only processes metadata such as:

- *table names*
- *column names*
- *monitoring metrics*

- *incident metadata*

Raw customer data values are not transmitted outside the Fabric environment.

Data Residency

Microsoft Fabric is making an Enterprise Promise around data not leaving the geography of the tenant for stored data and data in transit. As a workload in Fabric directly and users need to be aware what your commitments to Data Residency are. Define what your commitments are to the Data Residency of customer data.

Telmai is committed to ensuring customer data never leaves the customer's Fabric environment. The Data Plane queries data in place via the Analytics SQL endpoint, operating on behalf of the authenticated user using a delegated user token. Only calculated metrics are retrieved for monitoring purposes. No raw data values are fetched, moved, or transmitted to Telmai's Control Plane. Users retain full visibility and control over the queries being executed. Operational metadata (monitor configurations, incident records, tenant registry) is stored in Telmai's Azure-hosted Control Plane. For organizations with strict data residency requirements, an option exists to run the Data Plane entirely within the customer's own account. This configuration requires additional setup and engagement with the Telmai Sales team at sales@telm.ai.

Compliance

The publisher attests to the following security, data, and compliance regulations and standards

Telmai is architected to never move, copy, or store raw customer data outside the customer's Fabric tenant. Computed metrics retrieved by the Data Plane (such as row counts, null ratios, and schema fingerprints) are stored in Telmai's Control Plane for monitoring and anomaly detection. No raw data values or PII are stored in Telmai's infrastructure. All data in transit is protected via TLS 1.2 or higher. All data at rest is encrypted using AES-256.

Certifications and standards

- *SOC 2 Type 2 — certified, report available upon request*
- *GDPR — honored, data residency respected, regional backend provisioning supported upon request*
- *CCPA — honored, reflected in Telmai's Privacy Policy*
- *HIPAA — platform capabilities support customer HIPAA compliance requirements*
- *PCI — platform capabilities support customer PCI compliance requirements*

Supporting link

<https://www.telm.ai/product/security-and-compliance/>

Support

Live site

Partner workloads are an integral part of Fabric that requires that the Microsoft support teams are aware of how to contact you in case customers are reaching out to us directly.

Microsoft direct vendor outreach:

Contact Name/Team	Number	Email alias	Self-Service portal
Maxim Lukichev	+1 707-641-4995	support@telm.ai	https://telm.clearfeed.app
Hashem Raslan	+1 707-654-4094	support@telm.ai	https://telm.clearfeed.app

Supportability

Vendors are responsible for defining and documenting their support parameters (Service level agreement, contact methods, ...). This information needs to be linked from the Workload page and should always be accessible to customers. In addition, the Marketplace criteria, need to be taken into account for the listing of the SaaS offer.

- Vendor attests that support information is published to the marketplace offering and available to user/customers directly via the workload

Fabric Features

Application Life Cycle Management (ALM)

Microsoft Fabric's lifecycle management tools enable efficient product development, continuous updates, fast releases, and ongoing feature enhancements.

***Extra Requirements:*

- Supported
- Not Supported

CI/CD (Continuous Integration / Continuous Deployment)

The workload supports CI/CD pipelines to enable automated deployment and integration workflows within Microsoft Fabric.

****Extra Requirements:**

- CI/CD is supported via the Fabric CICD manifest section
- CI/CD is not supported

Describe any limitations or details about the CI/CD integration

Item Definition Portability

Items can be exported with their full definition and restored in other workspaces, enabling lifecycle management and cross-workspace deployment.

- Items can be restored with their definition in other workspaces
- Items cannot be restored in other workspaces

Telmai's Fabric workload surfaces as a MonitorSet item inside a workspace. Monitor configurations, asset registrations, incident records, and tenant registry data are stored in Telmai's Control Plane (Fabric SQL Database and KQL Eventhouse), not embedded in the item definition itself. Because the item definition does not carry the full configuration state, items cannot be independently exported and restored in a different workspace while preserving their monitoring setup. Cross-workspace portability of item definitions is not supported in this release. Customers who need to replicate a monitoring configuration across workspaces should work with Telmai support to migrate configuration state via the REST API.

Private Links

In Fabric, you can configure and use an endpoint that allows your organization to access Fabric privately.

- Supported
- Not Supported

Telmai's architecture separates the Data Plane (short-lived Spark container jobs running inside the customer's Fabric account) from the Control Plane (a Node.js hub hosted in Telmai's Azure environment). Because the Control Plane resides outside the customer's Fabric tenant and communicates with the Data Plane over REST APIs, Fabric Private Link configurations that restrict outbound connectivity from the

customer's tenant may prevent communication with Telmai's Control Plane. Private Links are not supported in this release.

Data Hub

The OneLake data hub makes it easy to find, explore, and use the Fabric data items in your organization that you have access to. It provides information about the items and entry points for working with them. If you're implementing a Data Item, show up in the Data Hub as well.

- Supported
- Not Supported

Data Lineage

In modern business intelligence (BI) projects, understanding the flow of data from the data source to its destination can be a challenge. The challenge is even bigger if you built advanced analytical projects spanning multiple data sources, data items, and dependencies. Questions like "What happens if I change this data?" or "Why isn't this report up to date?" can be hard to answer.

- Supported
- Not Supported

Sensitivity labels

Sensitivity labels from Microsoft Purview Information Protection on items can guard your sensitive content against unauthorized data access and leakage. They're a key component in helping your organization meet its governance and compliance requirements. Labeling your data correctly with sensitivity labels ensures that only authorized people can access your data.

Extra requirements:

For partners that are using Export functionality within their Item they need to follow the guidelines.

- Supported
- Not Supported