TM Forum Open APIs

Conformance Certification

Company Name: ***Jio Platforms Limited (B2C)***

TM Forum Open API Name:
TMF672 – User Roles and Permissions

TM Forum Open API Release Version: ***4.0.0***

Report Date: ***24/04/2025***

©TM Forum 2025. All Rights Reserved.

1. What Product or Solution does your API support?

JioID

JioID is a next-generation IAM product that offers a highly scalable, secure, and user-friendly authentication and access management solution. By leveraging advanced authentication techniques, robust session management, and seamless SSO, it helps organizations enhance security while delivering a frictionless user experience. With millions of identities to manage, this IAM solution ensures compliance, security, and operational efficiency across enterprise and digital ecosystems by enabling:

Unified Access

1. Develop a universal login system that allows users seamless access across all Reliance services and platforms.
2. Eliminate the need for multiple credentials, reducing user friction and improving convenience.

Enhanced Security

1. Ensure robust security protocols to protect user data and prevent unauthorized access.
2. Comply with global data privacy and security standards.

Scalability

1. Build a system capable of managing millions of concurrent users without compromising performance or reliability.
2. Enable integration with future Reliance services and third-party platforms.

User-Centric Design

1. Prioritize ease of use and accessibility, ensuring a consistent and intuitive user experience across devices and platforms.
2. Introduce features like biometric login and single-click account recovery.

© TM Forum 2025. All Rights Reserved.

2. Overview of Certified API

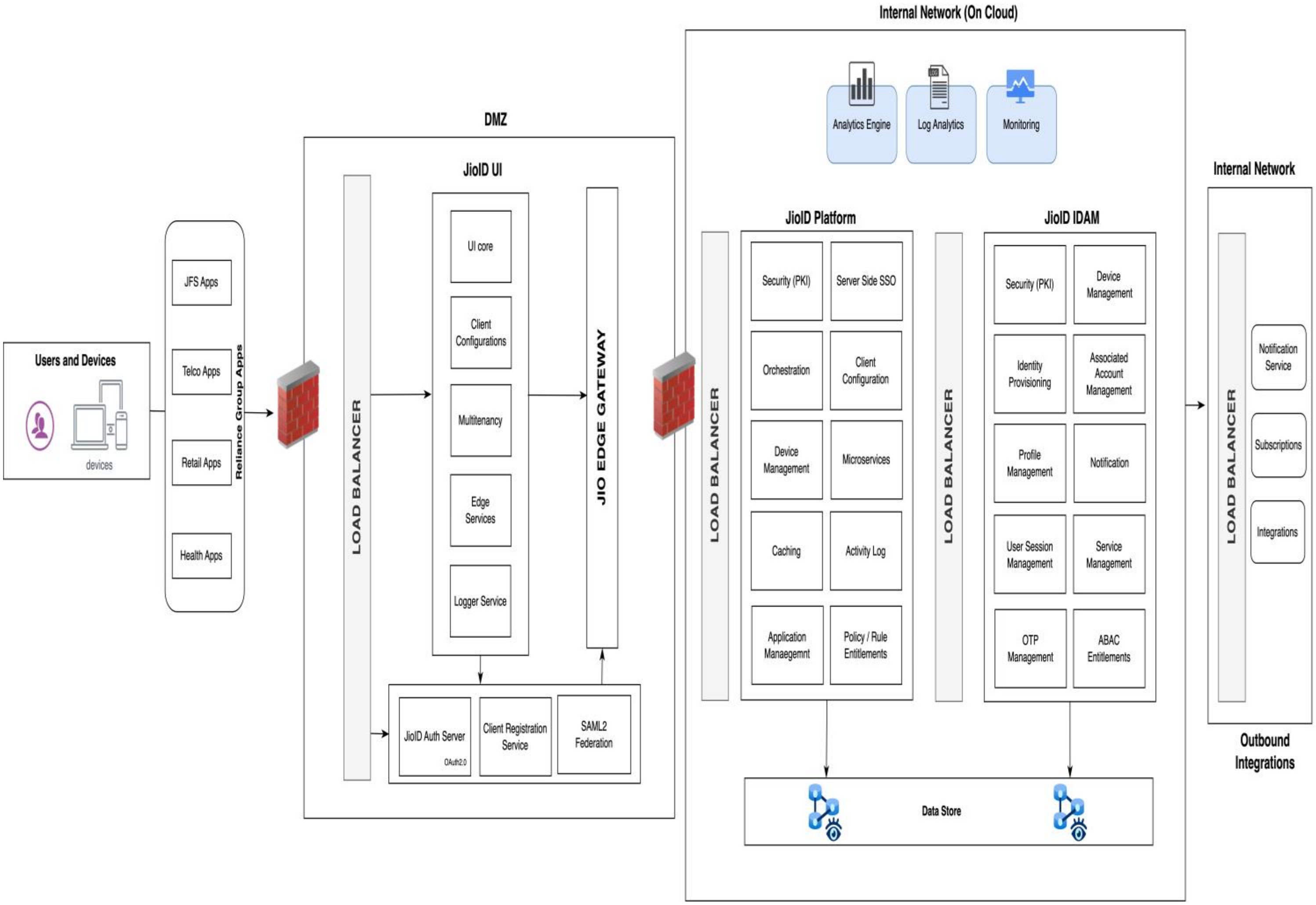
The Digital Identity and Role Permission Management API provides a comprehensive, standardized, and secure interface that enables enterprises to centrally manage digital identities, roles, and permissions across their digital ecosystem. Designed to work seamlessly together, these APIs ensure robust authentication, dynamic authorization, and strict compliance with enterprise security policies.

At the core, the Digital Identity Management capability allows client applications to manage the digital identities of individual customers, resources, and party roles, including authorized signatories. During the onboarding journey, each identity is automatically assigned a default role, establishing a foundation for secure and personalized access. This identity-centric model ensures seamless integration with downstream applications while supporting consistent identity resolution and lifecycle management.

The User Role Permission Management functionality enables system owners and administrators to define, manage, and assign roles and permissions efficiently. These roles, mapped to specific permissions (such as read, write, approve), govern what actions a user or resource can perform, thereby enforcing role-based access control (RBAC). The system ensures that each identity is granted only the necessary permissions aligned with their responsibilities—upholding the principle of least privilege access.

© TM Forum 2025. All Rights Reserved.

3. Architectural View



© TM Forum 2025. All Rights Reserved.

4. Test Results

Click here to view the test results: Jio-JioID-TMF672-HTMLResults.html

© TM Forum 2025. All Rights Reserved.