

# ForgeRock User-Managed Access (UMA)

*Enable Privacy, Consent, and Trusted Digital Relationships Across Cloud, Mobile, and IoT Sources*

Consumers have become hyper-aware of privacy invasions and they are all too willing to mistrust digital businesses. At the same time, they want new, personalized experiences such as incentives offered by geo-location or the ability to share their fitness data with their doctor. With data sources including not just web and mobile applications but also connected things, the pressure is increasing daily for organizations to secure customer data, address privacy regulations such as the General Data Protection law (GDPR), the California Consumer Privacy Act (CCPA), or the Consumer Data Right (CDR), and find ways to use that data to innovate and develop new digital offerings.

Consumers want to use new technology, but they also need assurance that their identity is being protected and shared in a responsible manner. Regardless of how good any new service is, adoption will suffer if customers feel that by using it, their privacy is being compromised.

Privacy and consent tools empower consumers by providing granular access controls for who can do what with their data, the ability to revoke their data at will, and the security needed to prove who is accessing their data. Organizations simply can't embrace digital transformation and comply with privacy laws without also delivering privacy and consent controls.

Giving customers, patients and citizens the context, control, choice and respect to securely and selectively share who gets access to their data helps build the trusted digital relationships needed to overcome privacy and consent challenges and grow the digital business. In order to achieve this, ForgeRock supports the User-Managed Access (UMA) standard.



## User-Managed Access Overview

User-Managed Access (UMA) is an OAuth-based access management protocol standard designed to give an individual a unified control point for authorizing who and what can get access to multiple sources of digital data, content, and services. UMA's federated authorization architecture is non-proprietary and resolves a host of access control, privacy, and consented sharing issues in today's API and IoT economies.

ForgeRock User-Managed Access, part of the ForgeRock Identity Platform™, gives users choice of who to share their personal data with, under what circumstances and for how long. It also helps organizations meet an ever-changing regulatory landscape while enabling robust application, mobile, and device ecosystems.

With a privacy and consent dashboard, users can delegate data access through a simple "share" button, and monitor and change sharing preferences at will through a central console.

For example, a patient collecting cardio data through a health wearable could stream data to a clinician to monitor heart rate, or collect and share that data with another doctor for a short time window in order to get a second opinion.

# ForgeRock User-Managed Access Key Features

## UMA Provider

---

**Fine-grained delegation and consent:** Gives end users a convenient central console for organizing digital resources residing in many locations, delegating scoped access to others, and monitoring and revoking access.

**Fine-grained access denial:** Provides a dedicated landing page for aggregating pending access requests; the end user can grant requests, edit down the scopes granted, and deny requests outright.

**Chained delegation:** Enables an end user who owns a resource to share it with another, who can in turn share it with another; the original owner can see the entire access history and disrupt the sharing chain by revoking the original policy.

**Dynamic policy enforcement point onboarding:** Lets each service used by an end user put their digital resources under central protection as the resources are created and changed.

**Security controls and usability features:** Lets an administrator set realm-level features such as access token expiration times and email notifications surrounding pending access requests.

**Customizability:** Lets implementers use extensive API endpoints and plug-in points to customize just about any characteristic of the UMA Provider, including replacing the standard XUI interface for the console.

**User-Managed Access (UMA) standard:** Provides conformance to the UMA standard for industry interoperability and easy application of the ForgeRock solution framework to the entire organizational or partner ecosystem, including federated authorization use cases as well as customer-centric use cases.

## UMA Protector

---

**Multi-service protection gateway:** Provides an enforcement point over any number of services or APIs, so that multiple UMA resource servers to which the end user has login accounts can be protected by the authorization server.

**Requester trust elevation for increased security:** Ensures that access requesters aren't just in possession of a "secret link" but goes above and beyond OAuth 2.0 in proving requesters identity, according to resource owner policy.

**Dynamic policy enforcement point onboarding:** Lets a web API register its digital resources with an UMA authorization server as those resources are created and changed.

**User-Managed Access (UMA) standard:** "UMAnizes" your web API, turning it into a conforming and interoperable UMA resource server that takes advantage of the UMA Provider's value-added features.

**"At Philips, we're on a mission to improve people's lives and to empower people to take better care of themselves and others. With the rise of cloud-based data, health and wellness apps and consumer sensors, it's important to be able to share all those sources of data with family members, health professionals and others under close personal control. With UMA, we are able to design innovative data-sharing and consent technologies into our HealthSuite Digital Platform that make it possible to foster consumer and patient trust."**

**JEROEN TAS**

CEO, Healthcare Informatics Solutions and Services, Philips

**PHILIPS**

## Why ForgeRock User-Managed Access?

ForgeRock believes securing the digital transformation journey requires a fundamental shift in how organizations approach customer identity and privacy. With ForgeRock, organizations can empower their customers, securely connect identities with the digital world, and provide new offerings that transform engagement without losing consumer trust.

ForgeRock supports the hardest UMA scenarios: those serving consumers, patients, and citizens as well as employees and partners. With an out-of-the-box user interface and a central sharing management console, organizations can leverage value-add features, such as share buttons, that let end-users choose to delegate selective access to IoT devices, online identity data, and other digital resources.

UMA provides the following business benefits to your organization:

- Improve, personalize, and secure customer experiences that drive loyalty and revenue.
- Enhance customer trust and mitigate new business and regulatory risks through a next-generation consent framework.
- Build digital ecosystems with third-party partners.
- Be viewed as trusted and gain competitive advantage.
- Ensure real-time accurate customer data.
- Utilize a common repeatable framework that enables consumers to easily and transparently authorize the conditions under which data collected by their devices is used and shared by others.

**“We’re also very confident that the ForgeRock Identity Platform and its implementation of the User-Managed Access (UMA) standard for privacy and consent, is the right solution for this challenge.”**

### **BILL YOUNG**

Identity consultant at the New Zealand Department of Internal Affairs



**Te Tari Taiwhenua**  
Internal Affairs

## Learn More About How UMA Can Help Your Organization

With full support for UMA, ForgeRock helps organizations build customer trust and unlock new opportunities.

**Contact us** or visit [ForgeRock.com](https://www.forgerock.com) to learn more.

### About ForgeRock

ForgeRock®, (NYSE: FORG) is a global leader in digital identity that delivers modern and comprehensive identity and access management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than 1300 global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit [www.forgerock.com](https://www.forgerock.com).

Follow Us

