

Control Access for People, Services, and Things

Our approach to access management? One system to download and deploy, with comprehensive access management capabilities to control access to all the things in your world, digital and physical. Say goodbye to integrating a grab bag of disparate products. Modern identity solutions need to take a platform approach, and reduce friction when dealing with people, services, and things, all while providing the highest possible security. A powerful identity platform can help companies use identity as the driver to create new revenue channels by helping them to create unique and innovative products and services.

To do this, the identity platform needs to deliver a dynamic and personalized user experience and to provide modern authentication methods moving beyond simple username and password, and fine-grained authorization to protect and secure resources. It must be able to provide identity and access services that are continuously secure, scalable, and can adapt to rapidly evolving demands.

ForgeRock Access Management, part of the ForgeRock Identity Platform™, provides the most comprehensive and flexible set of services required for customer identity and access management, as well as traditional access management capabilities. These services include advanced authentication, adaptive risk, intelligent authentication, mobile push authentication and authorization, contextual authorization, federation, single sign-on, social sign-on, basic self-service, privacy and consent, high performance session management, and OAuth 2.0 Proof of Possession.

Features & Benefits

Advanced and Intelligent Authentication

Endless authentication possibilities with over 30 out-of-the-box authenticators and authentication tree nodes to fit specific business needs.

Implement strong multi-factor authentication.

Quickly create dynamic customer authentication journeys across any platform.

Leverage user login analytics to increase user adoption rates, and improve the customer experience.

Easily configure and alter login journeys based on device, contextual, behavioral, user choice and risk-based factors.

Automatically redirect suspicious users for further monitoring.

Consume out-of-the-box authenticators, utilize existing authenticators, and integrate with cyber security solutions — all in one place.

Mobile Authentication and Authorization

Provide frictionless multi-factor authentication and

/HIGHLIGHTS

- » “All-in-one” access management, part of a comprehensive identity platform.
- » Easy configuration of authentication and authorization with the flexibility to manage people, services, and things.
- » Mobile authentication and push authorization, including passwordless logins and approvals, or frictionless multi-factor authentication using Push Authentication, with an easy to use mobile app for iOS and Android.
- » Fine-grained authorization and authentication, with real-time identity context that continuously assesses what the omnichannel experience should be throughout the user journey, as opposed to a one-time decision process.
- » Flexible architecture offering both stateless and stateful modes designed for the demands of large scale and elastic deployments such as DevOps environments with microservices, and Internet of Things (IoT).
- » Protection against token theft with OAuth 2.0 Proof of Possession support.
- » View and analyze logging and audit information across the platform using the Common Audit Handler, with support for the Elastic Stack.
- » Deploy on-premise or in the cloud, including AWS, Azure, and others.

password logins including Push Authentications with iOS and Android devices.

OATH and HOTP standards that allow one-time passwords on a mobile phone or other device to be used as an additional factor for authentication.

Enable consumers to securely and conveniently approve high risk transactions and events, via mobile phone notifications.

Adaptive Risk

Leverage contextual authentication to assess risk, invoking stronger authentication mechanisms only when necessary by evaluating who the user is and their context.

Authorization

Coarse and fine-grained authorization with fully customizable policies leveraging context and continuous security to deliver controlled access to resources using simple point and click, drag and drop operations.

Scripting can be used to extend logic during policy evaluation to any resource type, not only URLs but external services or IoT devices and things.

Federation

Leverage standards to deliver seamless federation across organizations.

Incorporate SAML2 federation into authentication chains, enabling the use of federated identities in stronger multifactor authentication scenarios.

Supports OpenID Connect which makes it easier and faster to build solutions requiring additional identity information.

Single Sign-On

Provide Single Sign-On (SSO) services for multiple resources on one domain, across domains, or even across organizations, allowing the use of just a single authentication credential to access all resources.

Enables a seamless heterogeneous OS and Web application SSO environment with Windows Desktop SSO support.

Social Sign-On

Accelerates user on-boarding using any social IDP that supports OpenID Connect or OAuth 2.0 such as Facebook, Google, LinkedIn, Instagram, VKontakte, and WeChat.

Session Management

Highly flexible session management enables both stateless and stateful sessions.

Stateless session management and autonomous servers allows for highly distributed elastic deployments with nearly unlimited horizontal scalability.

Stateful session management enables complex, multi-site failover environments to be always available to end-users with very high uptime.

Shared Services

The Common Audit Framework provides a means to log data consistently across the ForgeRock Identity Platform, and enables correlation of events and transactions. Audit topics, such as access and activity, can be configured independently delivering the data you want to the appropriate business services. Includes handlers for CSV files, JDBC connections, Syslog, JMS and Elasticsearch (part of the ELK stack).

Shared services can log and track transactions; used to build custom UIs; develop scripts using JavaScript and Groovy; and provide user self-services across the entire platform.

DevOps and Developer Support

Develop against the platform's common RESTful APIs that enable JSON or XML over HTTP, allowing access to all

the underlying authentication, authorization, and identity services. Also available Java & C APIs.

Leverage cloud automation and orchestration for push-button deployment and continuous delivery, with Docker support and powerful command line tools that integrate seamlessly into DevOps environments.

Security Token Service automatically translates protocols for providers who support different standards for federation and authentication.

Performance and Scalability

Support large-scale, highly available implementations with millions of users, tens of thousands of concurrent sessions, and thousands of authentications per second.

Leverage the embedded ForgeRock Directory Services as a configuration store, highly scalable and performant session-persistent token and user store.

Standards

All major federation protocols: SAML 1.x, SAML 2.0 (SP, IdP, ECP, and IdP Proxy), WSFederation (asserting, relying party).

Next gen-federation standards for cloud and mobile, including full implementation of OpenID Connect, OAuth 2.0, GSMA, and UMA 2.0, ensuring greater interoperability and consistent behavior for developers.

Export and import of policies via XACML.

ForgeRock Access Management is part of the ForgeRock Identity Platform, the only unified offering for access management, identity management, user-managed access, directory services, edge security, and an identity gateway, designed and built as a single, unified platform. The solution is built on a highly scalable, modular, extensible, and easy-to-deploy architecture. Context-aware capabilities enable your employees, customers, or citizens a personalized experience on any digital channel, whether a mobile device, connected car, home appliance, or whatever the next connected innovation might be.

/ABOUT FORGEROCK

ForgeRock®, the leader in digital identity management, transforms how organizations build trusted relationships with people, services, and things. Monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, Open Banking, etc.), and leverage the internet of things with ForgeRock. We serve hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, TomTom, and Pearson, as well as governments like Norway and Canada.

www.forgerock.com