FORGEROCK

/ACCESS MANAGEMENT

Purpose-Built to Seamlessly Manage Identities Across All Channels, On-Premises, in the Cloud, and on Mobile

Introduction

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, things and services, 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 rich and personalized user experience and to provide modern authentication methods like fine-grained and push authentication, moving beyond simple username and password, and fine-grained authorization to protect and secure resources. It has to be able to provide identity and access services that are continuously secure, scalable, and can adapt to rapidly evolving demands.

Identity and access management is going through a new golden age. CEOs are pushing growth as their top priority and digital innovation is the primary path to achieving growth. Identity is central to everything and, as a result, a foundational element to the digital transformation. Today's identity use cases, however, are quite different from classic, employee-centric identity and access management use cases, demanding a different type of identity platform focused on very different problems.

Legacy identity management solutions are based on monolithic platforms that use static rules to make decisions. Most of these offerings are "platforms" in name only, combining lots of standalone component products together under a single sales SKU. These solutions were not designed to easily integrate with any application (on premises or off), to provide secure device-agnostic access at all times, to handle large-scale populations such as what is needed for customer facing deployments, or to make decisions based on consumer context. In short, traditional identity management cannot meet today's business demands.

To connect customers and citizens to relevant goods and services in the digital age, businesses and governments instead require customer-focused identity management. They require a platform that can securely identity-enable new services in months not years, manage the identities of users' devices and the internet of things (IoT), support the massive scale required for consumer identities and machine-to-machine (M2M) microservices, and maintain a persistent identity across a multitude of devices and services. ForgeRock® Access Management delivers on all of these requirements, making it an ideal solution for users, administrators, and developers alike.

ForgeRock Access Management Overview

ForgeRock Access Management, part of the ForgeRock Identity Platform™, is a single, unified solution that provides the most comprehensive and flexible set of services required for consumer facing identity and access management as well as traditional access management capabilities.

What legacy identity vendors have traditionally delivered as several different products – single sign-on (SSO), social sign-on, adaptive authentication, strong and mobile authentication, federation, self-service, adaptive risk, web services security, fine-grained authorization, and so on – is delivered by ForgeRock as a single, unified offering. Organizations can use the access control services they need in a centralized way, and simply "turn on" additional services when ready.

The solution has a unique architecture to support use cases from complex consumer applications with devices and connected things, to multi-protocol federation, to enabling SSO for cloud systems, to enterprise access control, to securing machine-to-machine solutions using microservices. It is especially well-suited for external, customer-facing access requirements. At the highest level, ForgeRock Access Management consists of a single, self-contained Java application, service components such as stateful or stateless session management, client-side APIs and REST, service provider interfaces to enable custom plugins, and policy agents for web and access policies to protect web sites and web applications.

Organizations with existing internal access management solutions can easily integrate ForgeRock Access Management into their environment through API services or through the token translation service. Maintaining all installation and configuration capabilities within one application vastly simplifies deployment of new internally or externally facing services. In addition, agent configuration, server configuration, and other tasks are simplified so they are repeatable and scalable, making it easy to deploy multiple instances of the solution without additional effort. And with support for DevOps and dynamic cloud architectures, ForgeRock Access Management offers push-button deployment, enabling continuous delivery and elastic deployments that dynamically scale for demand peaks and troughs. The embedded ForgeRock Directory Services eliminates the need to configure a separate directory to support the configuration and user stores; if desired, users can utilize other directories such as Active Directory, DSEE or databases.

Key Features

Advanced Authentication

Supporting over 25 out-of-the-box authentication methods, and with the ability to create custom authentication modules based on the JAAS (Java Authentication and Authorization Service) open standard, ForgeRock Access Management enables you to determine the exact conditions in which a resource can be accessed, and to implement strong multi- factor authentication while keeping friction to a minimum. Scripts can be developed and easily integrated to augment authenticity validation by calling, for example, external identity verification systems. Windows IWA is supported to enable a completely seamless, heterogeneous OS and web application SSO environment. And these requirements can be enforced or exempted using the Adaptive Risk capability.

Intelligent Authentication

Intelligent Authentication is based on a powerful authentication tree framework that provides more flexibility, choice and security than traditional authenticators. Identity and security teams can easily configure, measure, and adjust multiple login journeys using digital signals including device, contextual, behavioral, user choice, analytics, and risk-based factors. With an intuitive drag-and-drop interface, you can quickly consume out-of-the-box authenticators, FIDO Web authentication, and integrate with cyber security solutions — all in one place. Unlike authentication modules, authentication nodes within trees are more granular and can have multiple outcomes rather than just success or failure. Provide deeper insight into how people and their devices interact with applications and services, improve the end-user experience, deliver dynamic personalization that goes beyond the login journey, and integrate with fraud detection systems to further prevent data breaches.

Mobile Authentication

ForgeRock provides flexible, simple to deploy, and easy to use mobile authentication, seamlessly integrated into the login process. Push Authentication enables secure, passwordless logins and frictionless multi-factor authentication. And one-time passwords provide even more ways to ensure the user is who they say they are. All of this can be implemented using the built-in authentication modules and ForgeRock Authenticator App, available for iOS and Android.

Adaptive Risk

Adaptive Risk is used to assess risks during the authentication process, to determine whether to require the user to complete further authentication steps. Adaptive risk authentication determines, based on risk scoring, whether more information from a user is required when they log in. For example, a risk score can be calculated based on an IP address range, access from a new device, account idle time, etc., and applied to the authentication chain. By using context to evaluate the legitimacy of the user's login attempt, ForgeRock Access Management can bar invalid entrants in real-time.

Authorization

ForgeRock Access Management provides authorization policies, from basic, simple, coarse-grained rules to highly advanced, fine-grained entitlements. Policies can be exported and imported via XACML. By externalizing authorization policy from applications and centralizing it within ForgeRock Access Management, developers can quickly add or change policies as needed, without modification to the underlying applications. Using a modern GUI-based policy editor with its point-and-click, and drag-and-drop operations, sophisticated policies can be built to deliver controlled access to resources. Developers can easily deal with fine-grained policies through REST APIs. For IoT use cases, universal authorization is used where solution-specific policies can be built with arbitrary resource types and custom actions, such as opening a door lock or switching on a light. Most access management solutions only assess risk at initial authentication. Contextual authorization with ForgeRock Access Management, on the other hand, allows for continuous security and dynamic, context- based policies. This allows organizations to assess risk not just at the time of authentication, but also as resources are accessed during the digital session. To gain greater knowledge about who the user is and what their context is, external policy information points can be called with easy to write scripts. Additional context can then be used to further assess risk, requiring stronger authentication mechanisms only when necessary. This makes the end user experience simpler while maintaining security by ensuring the authenticity of people, services, and things throughout the duration of each session. In addition, ForgeRock Access Management can act as a User-Managed Access (UMA) Provider for extensive privacy and consent capabilities, critical in helping to address evolving privacy regulations such as GDPR.

Push Authorization

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

first person based approval mechanism that is event based, increases security, and reduces the threat window for malicious activity. For example, an online bank user attempting to transfer money over a critical threshold to an existing payee would would trigger a mobile push notification, which the end user would approve using Touch ID or swipe. If the user attempted the same transaction only seconds later, the same approval would be required, to reduce malicious replay attacks. As more people and things come online, organizations need a simple way to manage them. To date, things like MFA have been primarily an authentication process. ForgeRock makes it an authentication and authorization process.

Federation

The federation services in ForgeRock Access Management can securely share heterogeneous systems or domain boundaries using standard identity protocols (SAML, OpenID Connect). This allows users to access services that span the cloud and mobile devices, on premises and off, eliminating the need for multiple passwords, user profiles, and the added complexity that frustrates users and slows adoption. SAML-based federation can be incorporated into authentication chains, enabling the use of federated identities in stronger multi-factor authentication.

Single Sign-On (SSO)

ForgeRock Access Management provides multiple mechanisms for SSO, whether the requirement is to enable SSO in a single domain, enable cross-domain SSO for a single organization, or enable SSO across multiple organizations through the Federation Service. It supports multiple options for enforcing policy and protecting resources, including policy agents that reside on web or application servers. The built-in Security Token Service (STS) can act as a multi-protocol hub, translating for providers who rely on other, older standards. A variety of flexible options for single sign-on are provided.

User Self-Service

ForgeRock Access Management is an ideal solution for customer-facing identity where it's essential to employ a light touch when dealing with millions of users, all while providing the highest possible security. Businesses need to deliver a great, easy- to-use self-service login, empowering the user wherever possible, such as through easy self-registration or password reset. Otherwise customers are very quick to go somewhere else.

Social Sign-On

ForgeRock Access Management supports social sign-on via social identity providers such as Facebook, LinkedIn, Google, Instagram, VKontakte, and WeChat, allowing users to login directly with their existing social accounts, thus paving the way for rapid customer adoption. In cases where you users should have accounts on your system, the Social Identity module of the ForgeRock Identity Platform can be added, giving full social registration capabilities. This lets users bring registration information such as name, email address, and so on, over from a social provider, significantly shortening registration time.

OAuth 2.0 Proof of Possession & Device Registration

The ForgeRock Identity Platform is an early adopter of the OAuth 2.0 Proof of Possession standard, ensuring that a token presented by a client (for example, a web browser accessing an application, or an IoT device connecting to a back-end system, and so on) is being presented by its rightful owner. This provides a transparent challenge/response-style interaction to prove the client is the intended owner of the access token and allows organizations to confidently create applications and services to meet their customers' needs, with less concern about token misuse from man-in-the-middle and other attacks.

In addition, device registration or pairing to particular services can be easily set up according to the de-facto standard OAuth 2.0 Device Flow, enabling companies to create unique product offerings that incorporate trusted devices and things.

DevOps and Developer Support

ForgeRock Access Management was designed from the beginning for interoperability and massive scale, ideal for customer facing deployments. Today, companies creating new products and services have embraced DevOps to achieve a faster time to market. With its DevOps friendly architecture, ForgeRock Access Management integrates seamlessly into continuous delivery environments, providing a comprehensive set of identity services to help companies generate new revenue streams and set themselves apart from the competition. With ForgeRock Access Management, organizations can leverage automation and orchestration for push-button deployment and continuous delivery.

Additionally, ForgeRock Access Management provides client application programming interfaces with Java and C APIs and a RESTful API that can return JSON or XML over HTTP, allowing users to access authentication, authorization, and identity services from web applications using REST clients in their language of choice. OAuth 2.0 also provides a REST interface for the modern, lightweight federation and authorization protocol. Features such as user self-service, policy, and security token service are also exposed through REST APIs, making it simple for developers to adopt powerful functionality. Widely used in mobile and web applications, OAuth 2.0 and OpenID Connect standards are more rigorously enforced, as the built-in OpenID Connect Provider is fully conformant with the OpenID Foundation's Conformance tests. This ensures greater interoperability and consistent behavior for developers.

High Availability and Scalability

With the advent of IoT, scaling identity systems has become even more challenging. Classic deployment scenarios involve stateful architectures where complex, multi-site failover environments offer extremely high reliability and uptime. And more recently, modern elastic cloud environments have allowed organizations to dynamically scale their production environment to meet demand peaks and troughs.
The ForgeRock Identity Platform can do both, with stateless and stateful session architectures that also enable "five 9's" availability for large-scale, mission-critical deployments. Stateless architectures are optimal for deployments with massive scale, into the hundreds of millions, and even billions of identities. With its Docker support and comprehensive remote configuration tools, ForgeRock Access Management is an ideal fit for these dynamic deployments. And for more traditional stateful architectures, ForgeRock Access Management provides both system failover and session failover. These two key features help to ensure that no single point of failure exists in the deployment, and that the ForgeRock Access Management service is always available to end-users. Redundant ForgeRock Access Management servers, policy agents, and load balancers prevent a single point of failure. Session failover ensures the user's session continues uninterrupted, and no user data is lost.

Common Auditing Architecture

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

Customer Use Case: Government of Norway

The Challenge

Deliver secure government services to Norwegian citizens and businesses so they can do things like obtain birth and death certificates, apply for schools and student loans, manage welfare services and health information, and pay parking tickets, automobile registration fees, utility bills, and taxes online.

The Solution

Implement a flexible, secure, single-access architecture built with ForgeRock Access Management to enable nearly 100% of all citizens to access over 300 government services.

How

The hub, ID-Porten, is at the center of the architecture. Government agencies such as the tax office, labor and welfare agency, health economics administration agency, and water and energy directorate are the spokes that use the authentication and single sign-on services of ID-Porten. The ID-Porten implements several levels of authentication: MyID, which uses PIN code authentication; BankID, a bank-issued electronic ID; Buypass, a private electronic ID that can also be used to bet online in Norway; and Certificates which are stored in USB pens and issued by a private company. Each of the authentication eIDs can be associated with different authentication contexts and different authentication strengths.

Benefits

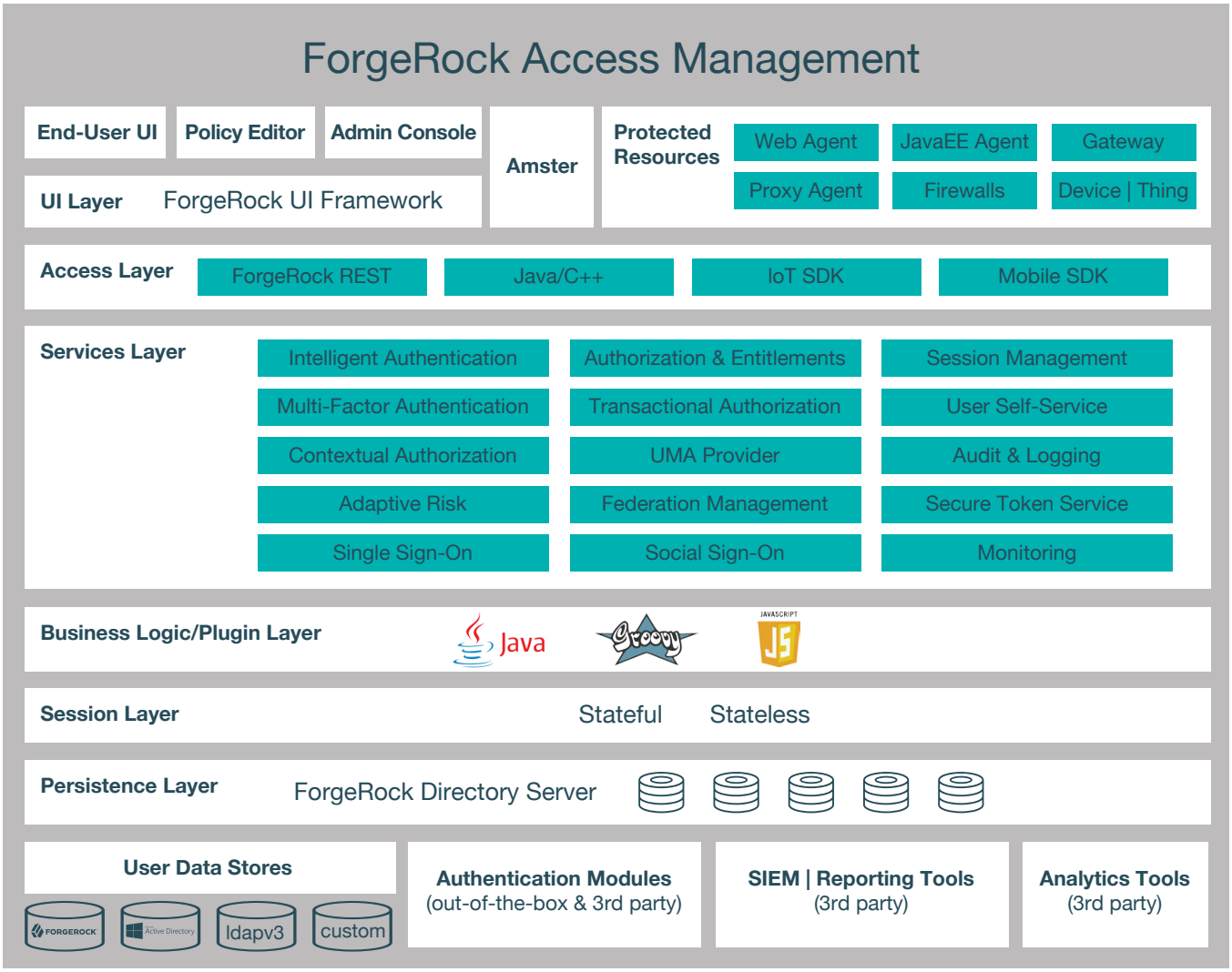
» Nearly 100% of adult citizens and over 500,000 businesses access municipal, regional, and national government services from a single portal online, resulting in ease of use, better security, faster processing times, and measurable savings.

» Scalabil ity and performance: ID-Porten and the authentication environment can handle more than one million users signing in on a single day without outages or degradation in performance, such as on the day taxes are due.

"ForgeRock Access Management's[1] simple, secure access to government services played a large part in the success of the eGovernment initiative."

- TOR ALVIK
COO, Agency for Public Management & eGovernment

1. ForgeRock Access Management was previously known as OpenAM.



Why ForgeRock Access Management?

ForgeRock Access Management is designed to give customers not only low friction, context-aware access, but also a personalized experience on any digital channel, whether a mobile device, connected car, home appliance, or whatever the next connected innovation might be. This can be achieved by putting identity at the center of all digital transformation projects and is enabled by the ForgeRock Identity Platform and ForgeRock Access Management.

ForgeRock Access Management provides the following key benefits to your organization:

Enables Solutions for Additional Revenue Streams

ForgeRock Access Management provides the tools and components to quickly deploy services to meet customer demand. For example, organizations can leverage user-login analytics within Intelligent Authentication to improve customer conversation rates. Additionally, the ForgeRock Access Management Federation Services support quick and easy deployment with existing SAML 2.0, OAuth 2.0, and OpenID Connect systems. For systems that do not support a full SAML 2.0 deployment, ForgeRock Access Management provides a Fedlet, a small SAML 2.0 application, enabling service providers to quickly add SAML 2.0 support to their Java or .NET applications. Simple OAuth 2.0 device registration and universal authorization, where IoT devices can be protected as easily as web applications, open up new possibilities for additional revenue streams.

Improves User Experience

ForgeRock Access Management enables users to experience more services using frictionless passwordless logins push authentication, the ability to choose how they want to login or what second factor they want to use through intelligent authentication, secure approval transactions using push-authorization, single sign-on without the need of multiple passwords,

"ForgeRock helped us integrate the ForgeRock Access Management2 solution into our highly complex, heterogeneous IT environment quickly and easily. In fact, the launch was so smooth that some users did not even realize it had taken place. The ForgeRock University team also provided training sessions to help our staff learn to use the solution quickly."

- MARTIN SCHIKOWSKI
Project Manager for Web Applications at Kabel Deutschland

social sign-on (e.g. with Google or Facebook accounts), and general user self-services such as registration or easy password resets.

Reduces Operational Cost and Complexity

ForgeRock Access Management can function as a hub, leveraging existing identity infrastructures and providing multiple integration paths using its authentication, single sign-on (SSO), and policies to your applications, things, or services, without the complexity of sharing web access tools and passwords for data exchange. ForgeRock Access Management can decrease the total cost of ownership (TCO) through its operational efficiencies, modularity, rapid time-to market, and high scalability to meet the demands of the customer- centric identity market. It's a single solution that offers SSO, social sign-on, advanced and intelligent authentication, federation, web services security, fine-grained authorization, privacy, IoT security, and more.

Easier Configuration and Management

ForgeRock Access Management centralizes the configuration and management of your access management system, allowing easier administration through its console and ForgeRock Access Management command line tools. The solution also features a flexible deployment architecture that unifies services through its modular and embeddable components. ForgeRock Access Management provides a common REST API, a common user interface (UI) model, and a common audit framework, providing scalable solutions as your customer base increases to the hundreds of millions, and also allows enterprises to outsource IAM services to system integrators and partners.

Increased Contextual Security

ForgeRock Access Management provides an extensive entitlements service, featuring attribute-based access control (ABAC) policies as its main policy framework with features like contextual authorization and authentication trees, import/export support to XACML, a policy editor, and REST endpoints for policy management. The ForgeRock Identity Platform also comes with an extensive common auditing service, including support for Elasticsearch in the Elastic stack, which allows organizations to view and analyze logging and audit information across the platform to monitor access according to regulatory compliance standards.

Conclusion

ForgeRock Access Management is part of the ForgeRock Identity Platform, the only 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, and Pearson, as well as governments like Norway and Canada.

www.forgerock.com