

Securely Manage the Complete Identity Lifecycle of People, Services, and Things

Introduction

Win over customers with a safe and secure online experience. Protection of user data, products, and services are more important than ever as we enter a hyperconnected world — it's a complex and extensive web of relationships, but that doesn't mean it has to be a mess. ForgeRock understands that as billions of people, services, and things, get online, you need better tools to manage and protect the relationships between them, at scale. ForgeRock Identity Management allows you to comprehensively and securely manage the complete identity lifecycle of people, services, and things. From identity to device registration, provisioning, synchronization, reconciliation, and more, your users and customers can feel safe as they move between devices and services. When your customers feel safe engaging with your products and services, and your critical assets are safe from harm, everyone wins.

Organizations of all sizes employ a variety of different approaches to manage identity administration and provisioning through the identity lifecycle. Traditionally

organizations only dealt with this process from the inside. However, organizations are dealing with the harsh reality of managing external users and identities as these users are looking to engage with the organization. The potential scale of external identities will outnumber the internal identities quickly, which leads to this dilemma: Is the current infrastructure used to administer internal identities capable of the large scale and special interactions required for external identity based registration and maintenance? To meet the need, organizations need to look at their identity administration and provisioning lifecycle differently than they have in the past.

Most consider identities to be people but as devices and “things” become more intelligent “they” also require identities. In terms of an organization, identity is no longer just a user and their computer but now a customer with many devices, or things like a thermostat managed through cloud services, traffic lights, citizen warning systems, cars, literally anything that is connected will need to be administered and provisioned.

This variety and potential veracity of registration needs will complicate the administration and provisioning as new devices, things, and services will put significant pressure on current infrastructures to scale beyond current levels. Organizations need to take an identity approach to engagement will remove barriers to entry that will improve how the organization interacts with customers and customers with the organization.

Organizations will soon quickly need to consider their current identity posture and plan for the future. Considerable consideration needs to be made to the infrastructure scale, identity administration and provisioning lifecycle and the level of engagement required to fulfill business needs. If all are accounted for properly, organizations could gain a considerable business advantage over their competitors.

ForgeRock Identity Management Overview

ForgeRock Identity Management, part of the ForgeRock Identity Platform™, is an identity administration and provisioning solution focused on managing relationships across people, services, and things, designed in response to the pain organizations suffer deploying legacy enterprise provisioning solutions. These mostly proprietary solutions are monolithic, heavyweight, painfully slow to deploy, and outrageously expensive; furthermore, they are not prepared for today's organizational needs, like connecting to cloud infrastructure and internet-connected devices and things.

Unlike legacy identity management solutions, ForgeRock Identity Management is a modular, plug-and-play identity service so you consume only what you need. In addition, it has a well-defined and simple REST API that is ideal for anyone in need of provisioning across enterprise, cloud, social, and mobile environments.

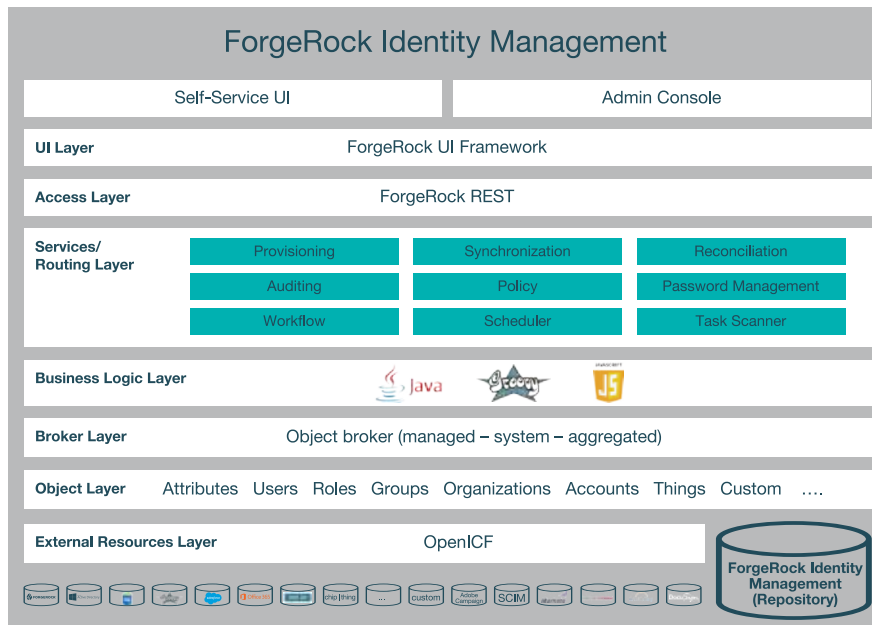
Utilizing a Java-based architecture that is built on the OSGi framework and therefore (See ForgeRock Identity Management Architecture) is able to provide lightweight, modular services such as automated workflow, user self-service, profile and privacy management, social registration, progressive profiles, password sync, data reconciliation, and audit logging, all accessible through developer- friendly REST APIs, using standard Java development tools such as Eclipse, NetBeans, Spring, etc.

ForgeRock Identity Management provides multi-layered provisioning activities through an embedded workflow and business process engine based on Activiti and the Business Process Model and Notation (BPMN) 2.0 standard. The modular design enables complete flexibility to use the embedded workflow engine and a database or replace these technologies with your selected platforms and services. Designed to have a small footprint, the entire service can itself be completely embedded and custom-tooled to the requirements of the target applications or services. Manage all of your identity sources: external systems, databases, directory servers, and other sources of identity through the built in identity connector framework, eliminating the need to rip and replace data stores.

Historically, the reason for building an internal enterprise user administration and provisioning system was to connect to the HR system. Now, organizations can support both internal employee systems and large- scale customer-facing applications. Configure the solution to create a virtual identity with links to external systems (data sparse model) or to create a meta-directory that centrally stores (data full model) a copy of identity attributes including virtual links to other external systems.

***“When it comes to identity management, legacy systems were not built with the modern world in mind. They were built for on-premises employees using a company-provided computer. As times have shifted to a multi-device-owning, always-connected mobile workforce, the complexity, cost, and potential for vendor lock-in of these legacy solutions has become increasingly apparent.*”**

- ESG LAB VALIDATION
ForgeRock Identity Platform



ForgeRock Identity Management Architecture

ForgeRock Identity Management provides workflow-driven identity provisioning for managing roles and entitlements assigned to people, services, and things. A modular architecture and framework supports extensive customization to address various business needs. Many areas of functionality can be adapted or extended through the use of simple scripts written in JavaScript or Groovy.

Key Features

Self-Service to Reduce Friction and Drive Customer Engagement

Being able to provide an easy, seamless registration, login, and password management service to end users is crucial for customer acquisition and retention. Self-service significantly reduces helpdesk costs and improves the customer experience by automating registration and password reset for millions of users. This enables admins to onboard and maintain customer and employee accounts with zero input and little customization required.

Profile & Privacy Management Dashboard – Build Customer Trust and Evolve with Regulations

Meet consumer demand and comply with continually evolving regulations with a transparent and centralized profile management solution. The Profile & Privacy Management Dashboard provides customers self-service for managing their personal info, password,

communication preferences, including the option for account deletion. Customers can also manage what personal data is shared with an external database, such as marketing automation platforms. Admins can also track and manage multiple versions of Terms & Conditions, or Terms of Service (ToS), and automatically prompt customers for their consent upon login when a ToS is updated. When combined with ForgeRock Access Management, the dashboard can be used to manage paired devices, applications, shared resources, and monitor activity changes made to the account.

Progressive Profiles

Customers prefer to share small amounts of information at a time. With Progressive Profiles, customers can register using simple, automated forms that progressively gathers information during designated moments of their journey. Easily build forms, gather additional profile attributes asynchronously, and enrich user profile data using automated policy-based rules. It's quick and easy for customers, and helps you gather more relevant, and accurate first party data.

Social Registration & Authentication

Accelerate and simplify registration and login by integrating social IdPs that supports OpenID Connect or OAuth 2.0, and non-standards based IdPs such as Facebook, Google, LinkedIn, Amazon, WordPress, Yahoo, Microsoft Live, Twitter, Instagram, Salesforce, WeChat, and VKontakte. This improves customer experience and helps you to build common user profiles for a centralized single view of the customer. By streamlining the registration and authentication process and consolidating social profiles customers can

conveniently use the same identity across applications and devices — a frictionless user experience for your customers. Within ForgeRock's Identity Management, developers can use simple configurations to quickly define scopes and gather specific user data for deeper insight into your customers.

Password Synchronization for Enforcing a Secure, Centralized Password Policy

ForgeRock Identity Management password synchronization, is a service that allows organizations to synchronize passwords in real time to ensure uniformity across all applications and data stores such as Active Directory. With password synchronization, any user, device, or connected thing authenticates using the same credentials on each resource.

Provisioning Based on Custom-Tailored Workflows

Leverage ForgeRock's Identity Management workflow and business process engine to create, read, update, and delete functions based on workflow-driven provisioning activities. Add workflows for self-service actions such as a user or device requesting access to an application, or an administrator handling bulk onboarding or off-boarding.

To simplify defining workflows and business processes, the embedded Activiti module can be used for modeling, testing, and deployment. Activiti is based on the standard BPMN 2.0 process definition models, which can not only exchange between different graphical editors, but can also execute as is on any BPMN 2.0-compliant engine. Organizations can easily custom-define workflows and business processes that meet their unique needs.

Least Privilege Security Model through Delegated Administration

Lower help desk costs and improve customer support by enabling administrator teams to assist with requests such as password reset. The ability to enforce fine and coarse-grained permission for users enables administrators to off-load daily tasks in order to better allocate time and effort. This improves the productivity of the workforce by ensuring minimal levels of access to applications, resources, and devices.

Delegated administration also helps organizations to improve their security posture by restricting users from having full administrator permissions which can expose critical assets and resources to data breaches.

Synchronization & Reconciliation - Simplifying the Identity Administration and Provisioning Lifecycle

In addition to passwords, ForgeRock Identity

“Initially, we considered traditional, closed source enterprise IAM vendors to help us drive our vision forward, but it quickly became evident that they would not be able to offer a solution that would be able to integrate or scale as quickly as we needed.”

- GREG KALINSKY

Senior Vice President and Chief Information Officer, GEICO

Management has the ability to sync and reconcile other attributes including role and group data between connected systems. ForgeRock Identity Management connector framework, allows provisioning to managed identities maintained by other identity providers. This connector framework provides a consistent coupled layer between resources and applications. These functions are critical to ensure that identity information is clean, consistent, and accurate throughout the connected resources. A flexible synchronization mechanism that provides for on-demand and scheduled resource comparisons is a key process for audit and compliance reporting. For organizations that provide services to users, devices, and connected things across multiple, disparate systems, streamlining identity management through synchronization and reconciliation services is essential to the identity administration and provisioning lifecycle.

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. In addition to the existing handlers for CSV files, JDBC connections, and Syslog, there are now two new handlers available: JMS and Elasticsearch (part of the ELK stack). When auditing is required, easy access to audit logs will take the pressure off IT organizations that need to demonstrate control and show infrastructure activities.

Connection to the Cloud without Complex Customization

With complete flexibility in data and object schema, the architecture of ForgeRock Identity Management enables support for both traditional on-premises applications as well as for cloud service based providers such as Workday, Google Apps, and Salesforce.com. Whether using the intuitive, out-of-the-box user

interface or the comprehensive REST API, it's easy to configure and capable of providing user provisioning and administration services to cloud providers without complex customization. As more and more services move to the cloud, it is important for organizations to simplify account creation, updating, deleting, and auditing without the cost and overhead of deploying multiple systems.

Flexible Developer Access for Unparalleled Customization

An open and well-documented access layer provides the user interfaces and public APIs for accessing and managing the ForgeRock Identity Platform, Identity Management repository and all its functions. RESTful interfaces provide APIs for CRUD operations and for invoking synchronization and reconciliation. The pluggable scripting engine provides interfaces to both JavaScript and Groovy out of the box.

User interfaces provide password management, registration, self-service, and workflow services. As organizations change, it's critical that their identity infrastructure changes along with them-which is why the open framework for developers is critical. An open framework provides developers with direct access to manage functionality at will.

Identity Data Visualization

ForgeRock Identity Management makes it possible to visualize identity relationships. Drill down on each node or object for more detailed information about each relationship. Admin dashboard widgets also enable admins to audit events and monitor IDM capabilities such as logins and registrations, system health, resource usage, and more. Additionally, gain a deeper understanding of managed identities by embedding reports built from the Kibana open source platform right into the management console. Build custom dashboards based on business requirements and easily share reports and dashboards with others.

Connectors

The ForgeRock Identity Platform data connectors are a standardized, out of the box way to connect and integrate third party identity repositories such as HR databases, eCommerce and marketing automation systems, directories, files, and XaaS providers. Popular connectors include SCIM, Marketo, Adobe Campaign, ServiceNow, Workday, DocuSign, Google, Salesforce, LDAP, and CSV file connectors. System connectivity is modular, extensible, and separate from the core engine. This results in reliable, low risk connectivity to different systems. Scriptable to enable connections to bespoke

APIs for data collection and bi-directional syncing, you gain exceptional flexibility to integrate, collect and synchronize data from many different sources, both modern and legacy.

Conclusion

ForgeRock Identity 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. With ForgeRock Identity Management, organizations can grow the business by connecting digital identities to new services while managing the identity lifecycle. For customers as they move from device to device, and they'll enjoy a seamless experience — on any digital channel, from Internet-connected things to traditional enterprise applications. ForgeRock Identity Management is the only 100% unified, lightweight provisioning solution that is also prepared for high scale and high volume. By providing enterprise features at internet scale, ForgeRock Identity Management provides identity administration and provisioning that is customized to fit organization's needs and requirements including role-based provisioning, high availability "out of the box," workflow synchronization (with delivery guarantees), customizable user interfaces, and password management.

For more information on ForgeRock Identity Management, click [here](#).

/ABOUT FORGEROCK

ForgeRock® is the Digital Identity Management company transforming the way organizations interact securely with customers, employees, devices, and things. Organizations adopt the ForgeRock Identity Platform™ as their digital identity system of record to monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, FCC privacy, etc.), and leverage the internet of things. ForgeRock serves hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, and Pearson, as well as governments like Norway, Canada, and Belgium, securing billions of identities worldwide. ForgeRock has offices across Europe, the USA, and Asia.

www.forgerock.com