

Federal Identity Credential and Access Management (FICAM) Capabilities and Strengths

Introduction

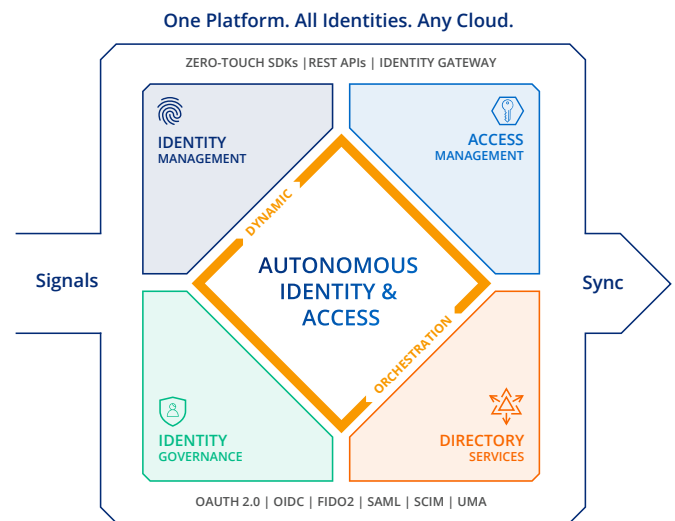
ForgeRock is a leading provider of identity and access management solutions. Its easy-to-use, AI-powered platform sets the standard for the industry. It manages over four billion identities globally and is deployed in all four major branches of the U.S. Department of Defense and many federal, state, and local government organizations.

Any government agency looking to modernize identity can use ForgeRock to design digital identity services that meet NIST SP 800-63-3, NIST SP 800-207, Executive Order 14028, and [GSA FICAM Services Framework guidelines](#).

The ForgeRock Identity Platform supports all major federation and authorization standards. It provides out-of-the-box capabilities for registration, user journey orchestration, single sign-on, (SSO), multi-factor authentication (MFA), passwordless authentication, zero trust architecture (ZTA), risk and identity management, and artificial intelligence and machine learning (AI/ML)-powered identity governance.

Hybrid/Cloud/No-Cloud: The One Solution for Every Environment

ForgeRock has a track record of delivering services at a large scale, using the same technology platform across different deployment architectures. This includes on-premises, private cloud, public cloud, or any combination thereof, at any Impact Level (IL2, 4, 5, and 6).



The ForgeRock Identity Platform is built for all person and non-person entities including consumers/citizens, workforces, internet-connected things, and APIs.

The platform is component-based, providing extensive functionality for greenfield services and applications, as well as legacy modernization and consolidation.

ForgeRock enables government agencies to create reusable service capabilities that will drive down the cost to deliver best-in-class FICAM experiences. The ForgeRock platform offers access management, identity management, user-managed access, directory services, and an identity gateway. Each component of the platform is designed and built as a single, unified solution for both enterprise users and customers.

Deployment for DevSecOps, Including Containerization

You can deploy the ForgeRock Identity Platform to any cloud (public or private) or data center using DevSecOps techniques like containerization and orchestration. Our Cloud Deployment Model (CDM) adheres to the [DoD Enterprise DevSecOps Reference Design](#) and demonstrates deployment in a containerized environment.

Your organization can take a true cloud-native approach to FICAM challenges by using CI/CD pipelines to protect your images, infrastructure, and workloads, as well as creating immutable microservices using Kubernetes and Docker containers. ForgeRock's data store is the only directory server in the industry that is a true, immutable microservice. It allows horizontal and vertical scaling both up and down without damaging the stateful data store. This architecture easily and seamlessly updates certificates without interrupting service. Many other vendors must go through a rigorous, off-line, manual process to update certificates.

Secured with Encryption, Hashing, and Zero Trust

You can configure ForgeRock to conform to Federal Information Processing Standard Publication (FIPS) 140-2 for encryption and hashing for in-flight messaging, protocol tunnels, and credential storage. ForgeRock is also certified in deployments against rigorous United States Department of Defense (DoD) Security Technical Implementation Guide (STIG) requirements and it can be deployed in IL6 and below environments. The platform also meets the NIST 800-20 Zero Trust standard for encryption at rest and in transit, least-privileged access, fraud detection, and many other requirements.

Agility, Scalability, and Availability for FICAM Use Cases

The ForgeRock Identity Platform allows you to build highly available, highly scalable services for 24x7 operations. It secures identity information for hundreds of organizations and governments — many operating global infrastructures supporting hundreds of millions of identities for customers and citizens.

The platform was built from the ground up to provide carrier-grade scalability and high-availability services to support your organization's or department's mission

requirements. ForgeRock's built-in capabilities, such as automated best-effort container placement, monitoring, elastic scaling, container orchestration, self-healing, load balancing, and configuration management, can be used with automated deployment techniques.

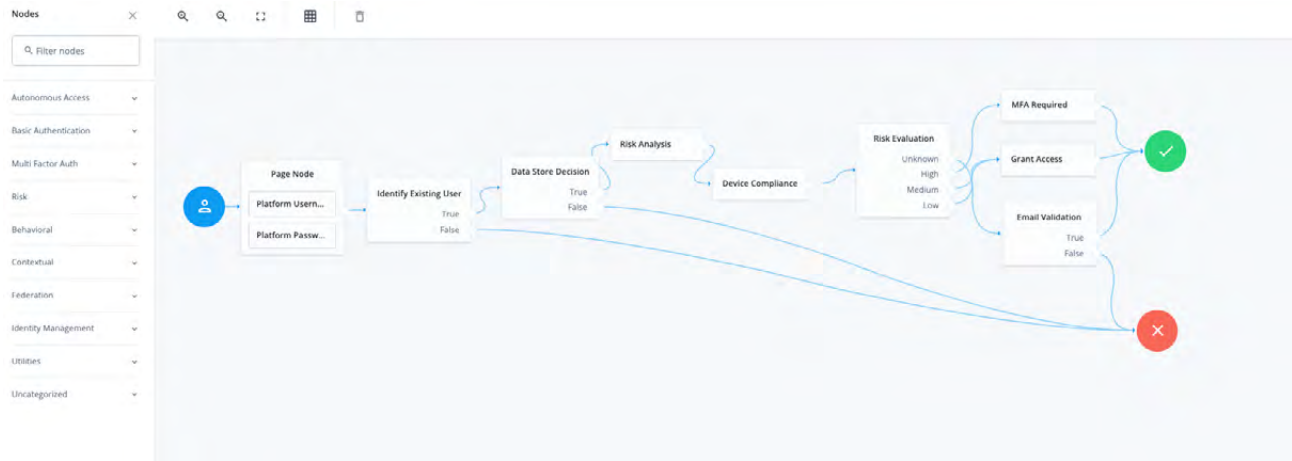
Flexibility to Support all Apps, Devices, and Identities

The ForgeRock Identity Platform is modular, lightweight, and highly flexible. The Pluggable-by-design architecture can adapt or extend behavior and functionality to meet FICAM requirements. The platform's component-based approach allows customers to build standards in a modular way to support all types of applications, devices, and person/nonperson identities (NPEs).

ForgeRock adheres to open standards, a modular architecture, and best practice design principles. ForgeRock products have gained a reputation for being extremely robust, highly scalable, and simple to deploy in any environment, spanning multiple data centers, platforms, and geographies. Your organization can quickly adopt new technologies, modernize legacy technology, and build business-critical platforms without vendor lock-in, all while using the same code base and DevSecOps framework.

You can deploy the platform entirely as its own ecosystem. It can function with or without connectivity, and synchronize when connectivity is restored. You can also design this ecosystem as part of a larger deployment and sync or share data if necessary. Numerous ecosystems can co-exist following a hierarchical model.

The ForgeRock Platform is a true microservices deployment. It can solve complex FICAM use cases around denied, degraded, intermittent, or limited (DDIL) communications in both classified Secure Internet Protocol Router Network (SIPRNet) and Non-classified Internet Protocol (IP) Router Network (NIPRNet) enclaves.



Authentication, Authorization, and Orchestration

The ForgeRock Access Management module provides the most comprehensive and flexible set of services to meet today's FICAM requirements. ForgeRock Access Management orchestrates and manages access at scale for any use case, including workforce, citizen, IoT/NPEs, and APIs.

When considering Zero Trust security models, it is no longer sufficient to use one or two authentication factors — even if these are strong AAL3 authenticators. Adaptive authentication using additional signals such as contextual, behavioral, and risk-based factors must also be considered. With ForgeRock, organizations can define their MFA options, risk-based access control, and federated access management.

ForgeRock Intelligent Access is the drag-and-drop visual design interface in ForgeRock Access Management that simplifies the process of configuring, measuring, and adjusting user journeys using device, contextual, behavioral, user choice, analytics, and risk-based signals. You can use Intelligent Access to administer more secure, risk-aware authentication scenarios while maintaining a low-friction login experience. Intelligent Access orchestration provides workflow-like decision trees that you can easily view, create, change, and dynamically configure using a drag-and-drop interface.

You can design authentication journeys to include step-up authentication, physical and behavioral biometrics, and Zero Trust policies. The nodes within a tree can incorporate location, IP address, device type, network, or any other contextual information that is included in the request and/or provided by third-party tools. Based on the outcome, you can configure nodes to calculate risk, modify the authentication level, alter session properties, and more.

Identity Management for Tailored Customer Experiences

The ForgeRock Identity Platform handles different types of identities in the same way. These can be internal users, external users, mobile devices, and nonperson entities. You can map any identity profile attributes to a session and make them available to a protected application via either a policy agent, ForgeRock Identity Gateway, or API/REST. This flexible attribute model enables granular access control decisions for web or other resource types. You can also group identities into realms that logically partition isolated environments.

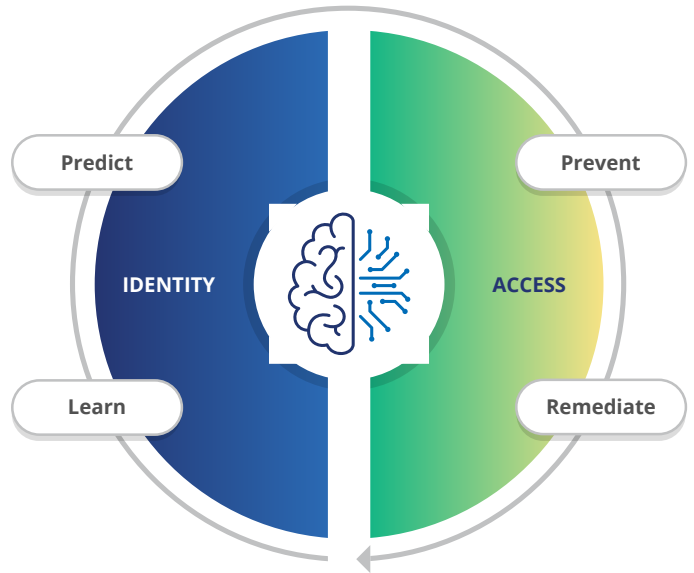
ForgeRock Access Management realms can have separate user data stores, authentication settings, authorization policies, administrators, and user interface (UI) branding. The platform provides a single centralized place to define key elements of the customer journey.

You can configure authentication centrally and enable it across all channels through an easy-to-use API. You create a unified and frictionless user experience regardless of whether people interact with your systems using a smartphone, laptop, kiosk, or any other device. At the same time, you can customize user journeys to the individual based on their specific attributes.

Trust and Zero Trust

To achieve Identity and Authentication Assurance levels (IAL 1-3 and AAL 1-3), you need to establish a level of trust for the user's identity and their devices. ForgeRock supports security frameworks for privacy, compliance, Zero Trust, and continuous adaptive risk and trust assessment (CARTA). Agencies have mandates to ensure only authorized employees have access to federal information systems. They require a higher level of assurance following the HSPD-12 Personal Identity Verification standard (PIV/CAC).

The ForgeRock platform supports easy integration into a PKI infrastructure and new technology like FIDO2 WebAuthn for easy authentication in both mobile and desktop environments. It leverages AI and ML to provide a greater level of understanding of access and behaviors. The platform also helps organizations radically improve and scale all things identity, governance, and access management with the industry's only full-suite, AI-driven platform.



Conclusion

There are many strengths and differentiators that separate ForgeRock from other vendors' offerings. If you are looking for a DevOps-friendly, low-code/no-code, flexible and scalable FICAM solution, give ForgeRock a try.

We are a leader in the Gartner Magic Quadrant for consumer/citizen identity and access management (CIAM) and Access Management. We offer free dev and test environments and have an attractive licensing model no matter the number of applications or enclaves/domains you need to manage.

ForgeRock can help you achieve Zero Trust in a frictionless easy-to-deploy solution. Our modular approach and standards-based design allow you to implement the latest authentication standards and provide a future-proof, adaptable solution for current and future needs.

About ForgeRock

ForgeRock® is a global digital identity leader helping people simply and safely access the connected world. The ForgeRock Identity Platform delivers enterprise-grade identity solutions at scale for customers, employees, and connected devices. More than 1,300 organizations depend on ForgeRock's comprehensive platform to manage and secure identities with identity orchestration, dynamic access controls, governance, and APIs in any cloud or hybrid environment. For more information, visit: www.forgerock.com

FOLLOW US

