

# ForgeRock Identity Cloud Packages for Workforce

The ForgeRock Identity Cloud is the market's first comprehensive identity platform as a service. Built for organizations looking for a comprehensive, enterprise-grade identity platform, Identity Cloud delivers usability, customizability, and operational cost savings. It is packaged to meet your enterprise business needs. You can start your Identity Cloud journey with the Core package and add supplemental packages as needed.

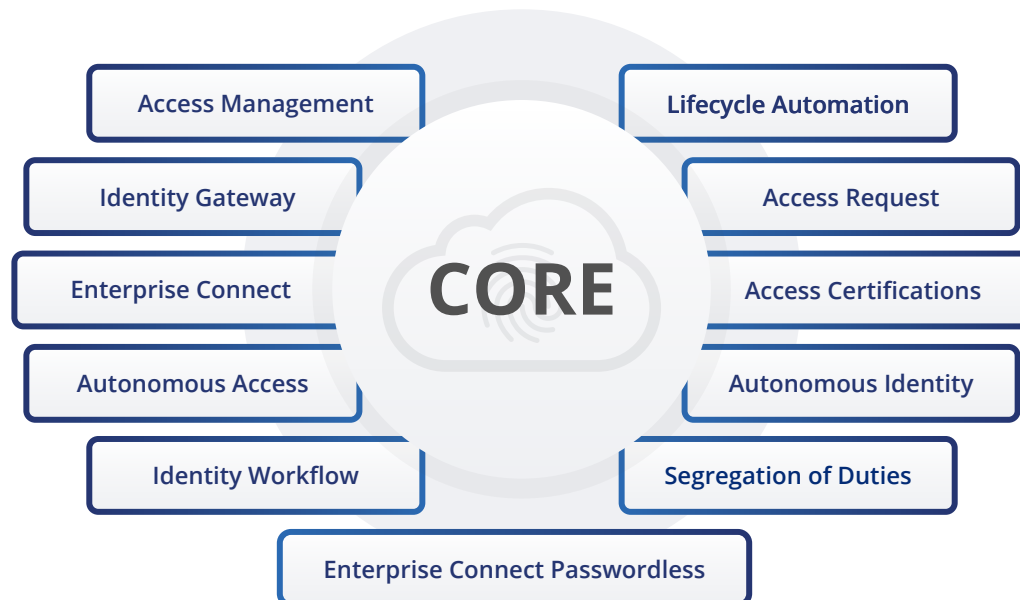
## Identity Cloud Packages

### Core

The ForgeRock Identity Cloud Core package provides industry-leading technology essentials to meet the demand for superior digital experiences. The Core package is designed to solve your foundational workforce identity and access management needs. It includes the ability to quickly discover new joiners, movers, or leavers (JML) from authoritative sources like your human resources (HR) systems to determine user access privileges and centralize your user identities in the cloud. Core includes user

authentication with a simple-to-use password mechanism and federation from third-party service providers to allow users to login to Identity Cloud. Core also features user self-service capabilities to reset or change their passwords, easily reducing your helpdesk service costs.

To address additional requirements, the Identity Cloud Core package can be customized through upgrade packages: **Access Management, Identity Gateway, Enterprise Connect, Enterprise Connect Passwordless, Autonomous Access, Autonomous Identity, Lifecycle Automation, Access Request, Access Certifications, Access Request, Identity Workflow, and Segregation of Duties.**



## The ForgeRock Identity Cloud Product Packages

## Access Management

The Identity Cloud Access Management package provides increased security while improving user experience with capabilities, such as single sign-on (SSO) to multiple applications, as well as adaptive and multi-factor authentication (MFA). It also provides strong authentication factors, including passwordless authentication using WebAuthn, FIDO, one-time passcode (OTP), email confirmation, mobile push, or magic link. Additionally, organizations requiring more contextual and fine-grained authorization enforcement components can leverage Access Plus to enforce continuous and contextual authorization for transactions. Access Management also includes dynamic scopes and continuous risk monitoring capabilities.

## Identity Gateway

The Identity Gateway package extends the security capabilities of ForgeRock Identity Cloud to legacy applications on-premises and to modern microservices running in the cloud. Identity Gateway enables Identity Cloud to coexist with legacy IAM solutions and augment legacy or home-grown applications with modern IAM capabilities, giving you time to execute on your cloud migration and security strategy. ForgeRock Identity Gateway includes capabilities to create a secure perimeter for modern API traffic and microservices.

## Enterprise Connect

The Enterprise Connect package delivers desktop single sign-on (SSO) and workstation multi-factor authentication (MFA) for your workforce infrastructure. With a single workforce MFA solution, you can stop credential-based attacks and provide more secure access to business apps, systems, and services. It also includes remote desktop MFA to ensure secure access for virtual and remote Windows desktops. To support your hybrid workforce, Enterprise Connect enables you to secure your VPNs and other legacy applications, such as databases and Unix/Linux servers using Radius.

## Enterprise Connect Passwordless

The Enterprise Connect Passwordless package enables you to embrace passwordless using a range of passwordless authentication methods, such as FIDO2 WebAuthn, passkeys, OATH, push, OTPs, biometrics, and more. The package includes no-code access orchestration so you can quickly configure and deploy drag-and-drop passwordless authentication workflows, and you can add security signal analysis and third-party integrations based on your organization's security and user experience needs. Using its application integrations, you can ensure simple and secure passwordless enablement for enterprise applications and infrastructure, including legacy applications, Windows and Mac workstations and servers, RADIUS-based

authentication, Remote Desktop (virtual and Windows), desktop SSO, VPNs, databases, mainframes, LDAP, REST, and Unix/Linux servers, and much more.

## Autonomous Access

The Autonomous Access package leverages a unique combination of AI, machine learning (EUBA), advanced pattern recognition (heuristics), and big data to provide risk scores to help stop known bad actors, flag anomalous behavior, and learn about new and emerging cyberthreats. Built into ForgeRock Intelligent Access, it includes out-of-the-box threat protection nodes and drag-and-drop configuration, making it easy for your teams to create any number of personalized user access journeys based on identified risk scores. By verifying and securely authenticating all your workforce users, you can achieve the goals of security, privacy, experience, and compliance as defined by a Zero Trust or CARTA framework.

## Lifecycle Automation

The Lifecycle Automation package includes a full-featured outbound provisioning and deprovisioning engine with bi-directional synchronization. Lifecycle Automation reconciles application accounts seamlessly to ensure that user identity data, including passwords, are always up to date. It ensures that you have a secure application environment where all identity data is consistent across all systems. Lifecycle Automation also includes password synchronization plugins for Active Directory (AD) and an LDAP server (including ForgeRock Directory Services) to ensure uniform password changes across all identity repositories. Lifecycle Automation also enables you to easily move from an existing on-premises service to Identity Cloud by providing pass-through authentication that validates passwords with a remote service along with the ability to migrate user identity as part of the authentication (just-in-time migration).

## Autonomous Identity

The Autonomous Identity package delivers an artificial intelligence (AI)-driven identity analytics solution that leverages machine learning (ML) techniques to collect and analyze identity data and identify access blind spots during access review and access certifications. With Autonomous Identity, you can eliminate over-provisioning by automating access approvals and reviews. You can also leverage ML to analyze and discover role access patterns across the entire enterprise. Role owners or role engineers can review, evaluate, and visualize existing roles and role models. This helps the organization optimize the existing role model and create fewer but higher quality roles.

## Access Certifications

The Access Certifications package enables organizations to perform periodic access certifications or access reviews to ensure continuous compliance, least-privileged access, and a Zero Trust security model. Certifications can also be generated ad-hoc when there is an organizational transformation or when a user changes roles to ensure that the access levels are still appropriate. When combined with Autonomous Identity, Access Certifications can accelerate manager access decision making with high-initiative access review campaigns embedded with AI-determined access recommendations and confidence scores.

## Access Request

The Access Request package empowers users with a 24/7 self-service access request portal along with an access request catalog. This package provides application owners or user managers an easy-to-use approval inbox to review all of the requests waiting for approval. When combined with Autonomous Identity, Access Request can provide recommendations on what application(s) users should or should not have access to.

## Identity Workflow

The Identity Workflow package automates the identity lifecycle processes with pre-configured, no-code identity orchestration workflow templates. The identity workflows enable you to quickly tailor activities such as user requests, approvals, escalations, and integrations to external systems. This package eliminates manual, error-prone processes and custom coding with a drag-and-drop graphical editor to rapidly design and personalize workflows to fit your business needs.

## Segregation of Duties

The Segregation of Duties (SoD) package enables least-privileged access security and a Zero Trust security model by applying and enforcing separation of duties. These SoD checks can be performed as preventive and detective checks to ensure security best practices and compliance with internal controls and regulations. The preventive controls can be enforced during user access requests so that a user cannot request roles or entitlements that conflict with something they already have. The detective controls can be evaluated ad-hoc or during certification to identify rogue accounts and inappropriate user access.

# Get Started With the Identity Cloud Package That Fits Your Needs

ForgeRock Identity Cloud packages give you the usability, customizability, and operational cost savings required to meet your unique goals and requirements today as well as tomorrow.

Contact us today to learn more and get started.

### About ForgeRock

ForgeRock® (NYSE: FORG) 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](http://www.forgerock.com).

### Follow Us

