ForgeRock®

How To Migrate from Oracle® Access Manager to the ForgeRock® Identity Platform

The Identity and Access Management (IAM) landscape has drastically changed in recent years. It has transcended beyond the enterprise, beyond the DMZ into the cloud, into devices, and now even into chips. Traditional Web Access Management (WAM) systems like Oracle® Access Manager were designed to solve problems limited to the confines of an enterprise and its employees, mostly catering to use cases around web based single sign-on (SSO) and coarse grained (URL) policy enforcements. Today's current landscape, SSO is just one of numerous critical services that you need to provide to your employees and customers in order to remain productive and competitive. Traditional and legacy products have fundamental gaps that will inhibit your business from achieving next generation services and security that digital transformations mandate. For example, a legacy WAM system like Oracle Access Manager:

- Is not agile enough to keep up with today's quickly changing business requirements, affecting your ability to go-to-market, reduce costs, and provide your customers with cutting edge technology.
- Was designed decades ago and has bolted on features.
- Lacks both modern architecture and functionality and, as such, were not designed to be deployed globally without incurring huge infrastructure and operations cost.
- Assumes that identity can only belong to a person or groups and hence cannot deal with any abstract identity or object such as devices nor the relationship between persons, groups and objects.
- Lacks major features to support Customer Identity and Access Management (CIAM) scenarios such as social registration and account linking (Oracle Access Manager in particular).
- Lacks support for the User Managed Access (UMA) standard, a protocol that enables consumers to securely share their data with another person while maintaining control over it.
- Lacks the major features to support Enterprise Identity and Access Management (IAM).
- Lacks Fine Grained Authorization, support for RADIUS (for VPN Access), DevOps for cloud deployment and even capabilities like Secure Token Services for exchanging tokens (Deprecated in the newer releases (Oracle Access Manager in particular).
- Lacks a comprehensive REST API and as such cannot be used with non-web-based applications such as mobile, microservices, and other types of devices.
- Requires multiple add on products, 3rd party databases, and extensive customizations for additional features, thus adding to the cost and complexity of the solution and time to market.
- Was designed to work in silos and not as a singular solution (integration between Oracle's own products, whether through mergers or acquisitions of other vendors and products, is an investment in itself).

As more people, devices, and things are assigned identities across networks, IAM services that are simple, flexible, scalable, and designed to quickly verify identities and access privileges become imperative for any business to safely and efficiently engage with their employees and customers. Beyond users' identities, today's solutions must also link devices—laptops, phones, touchpads, cars, wearables—and new mobile and social apps to a single security platform that works all the time, everywhere, on premises or off in the cloud. The ForgeRock® Identity Platform™ is designed with this new reality in mind.

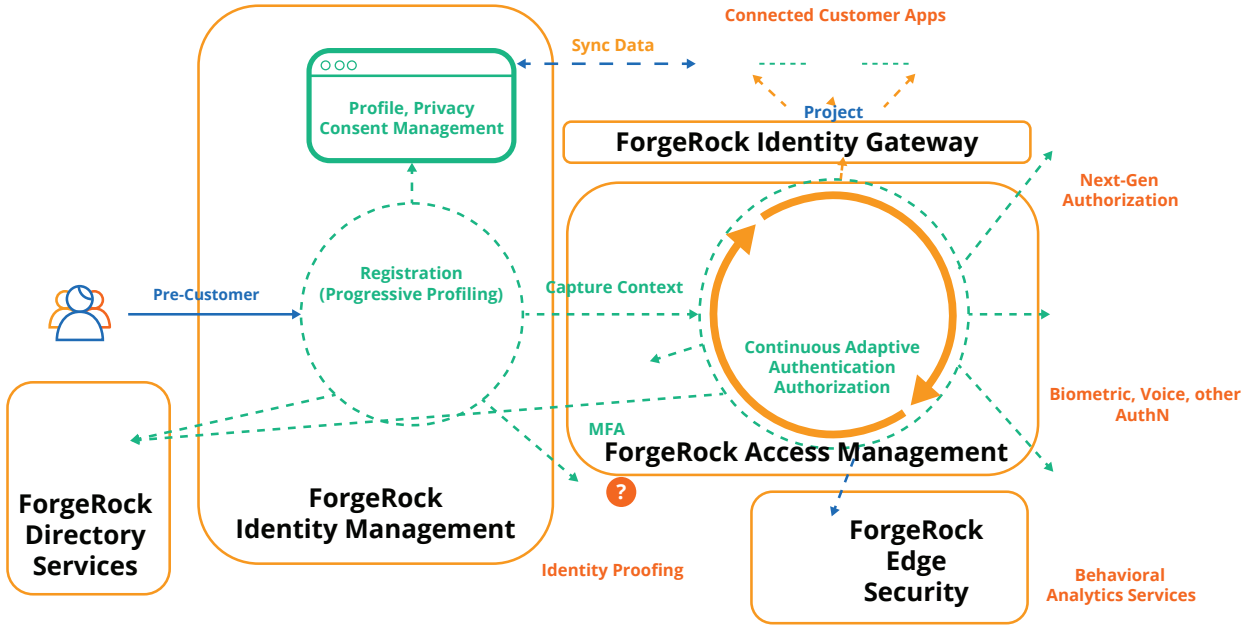

Diagram 1: The ForgeRock Identity Platform Offers Complete IAM for Today and Tomorrow's Use Cases

ForgeRock offers the most simple and comprehensive Identity and Access Management Solution to help our customers deepen their relationships with their consumers, and improve the productivity and connectivity of their employees and partners. ForgeRock was the first identity vendor to offer an agile, all-in-one, unified platform for rapidly building identity services that are lightweight, modular, massively scalable, and developer-friendly. Not only can a single deployment cater to your internal employee needs, but the platform can also be used for the internet of things (IoT), microservices, and external entities, including customers, patients, and citizens. The ForgeRock Identity Platform is architected to work as a unified solution well into the future, designed to deliver secure and trusted digital relationships at scale and with privacy-by-design principles that improve user experience, and, ultimately drive greater value and revenue.

The ForgeRock Identity Platform can easily cover traditional WAM scenarios, but also provides modern and cutting edge features as illustrated in the Key Focus Areas figure above. Key features and capabilities of the ForgeRock Platform include:

- Multi-tenancy, which enables you to segregate internal and external use cases without the need to install and manage different deployments. If a single deployment can cater to both internal and external audiences then the footprint of the deployment is reduced, with substantial savings in cost of infrastructure and operations.
- It has been designed to strike a balance between security and the user experience ,such as Multi-Factor Authentication and Authorization, yet reduces the friction that higher securitytypically brings to the end user by allowing for passwordless (push) authentication for a seamless experience.
- It based on common services that exposes configuration, management, services, and standards via a comprehensive REST API. Most other vendors provide an API that is limited to OAuth 2.0 only and hence restricts developers and integrators to write proprietary code to integrate with your applications.
- ForgeRock is an early adopter of emerging open standards and was the first identity provider to adopt new standards such as OAuth 2.0 proof of possession and User-Managed Access (UMA).
- It can be deployed on-premise, in the cloud (including multi-cloud and bring-your-own-cloud), or as a hybrid model. Additionally, the ForgeRock platform is DevOps friendly so it can be deployed in the cloud as a Kubernetes cluster or other clustering and container technologies such as Docker.
- Its components are all 64-bit, multi-threaded, IPv6 compliant and are built with modern software engineering practices, policies, and tools. The ForgeRock Identity Platform is not only horizontally and vertically scalable, but is also very secure. White hat testing and rigorous code reviews are a critical part of the engineering process.

As with adopting any new technology, it is useful to draw parallels to the concepts that you are already used to. The next section provides a comparison of the fundamental features and terminology between The ForgeRock Identity Platform and Oracle Access Manager. It should be used to compare the architectural similarities and differences from the point of view of migrations.

Migrating to Oracle® from Access Manager

The following section outlines the key concepts between ForgeRock and Oracle Access Manager architectures, including coexistence when migrating to ForgeRock. High level methodology and the steps needed to perform a migration are included. It is important to note that the migration described in this paper is for a complex Oracle Access Manager deployment. If your deployment is straightforward and you are only using it for scenarios such as single sign-on and a few policies, the migration will be shorter and simpler.

Concepts Comparison

ForgeRock Access Management (AM) has very similar concepts and components to Oracle Access Manager but in the form of a much more modern platform. For example, there is a policy engine (server) with policies that comprise of resources. AM has Policy Agents much like Oracle Access Manager WebGates that can work both in reverse proxy as well as be deployed on containers and managed centrally. It has a session store as well as sessions based on cookies. User profile attributes can also be retuned as headers and their names can be mapped to match your existing headers in Oracle Access Manager. All of these similarities help ease not only the transition to a modern solution, but also help make the transition smoother as the learning curve is smaller. In other words, unlike some other vendors, ForgeRock does not force a completely different solution, but allows you to gradually transition to a modern solution while keeping your legacy applications running smoothly, without touching them or forcing you to make changes to your existing environment. The ForgeRock Identity Platform also provides stateless sessions in the form of JSON Web Tokens (JWT). This is particularly useful for Customer Identity and Access Management (CIAM) use cases, such as very large scale deployments

Component Level Concepts

ACCESS SERVER (PDP)

AM Server (PDP)

An autonomous AM server is a PDP as well as PAP.

WEBGATE (PEP)

AM Web Policy Agents
AM J2EE Policy Agents
Identity Gateway (IG)

AM provides agents for all platform containers by Oracle Access Manager and more.

DATA STORES

POLICY STORE

USER STORE

KEY STORE

DJ Server
AM Server

AM has the same concepts of Policy and User Store. AM is not limited to a single user store and can be pointed to multiple user stores where the same user can reside thereby improving your integration experience.

Component Level Concepts *Continued*

SESSION STORE

AM Server (CTS)

The AM Core Token Service (CTS) stores persistent sessions and other token types such as OAuth2 tokens. The underlying repository of this store is DJ. This means that you don't need to setup an Oracle Database environment just to run your AM deployment.

ADMINISTRATIVE UI

AM Server

The Admin UI is not a separate component but part of the AM Server. However, for additional security we provide a headless (without UI) server.

Oracle Identity Federation (OIF)

AM Server

If you are running older version of Federation and have a separate installation of OIF, you can safely decommission that after migrating to AM as it is an integral part of AM and no separate component is required.

ADAPTIVE AUTHENTICATION SERVICE IN 12C

OR THE DEPRECATED ORACLE ADAPTIVE ACCESS MANAGER INTEGRATED WITH OAM IN 10G OR 11G

AM Server - Intelligent Authentication (Adaptive Risk Based Authentication) and Authorization

Fingerprinting devices is part of AM Adaptive Risk Scoring and is a standard feature. Not only can AM do risk evaluation during authentication, but any time after the fact. Context is evaluated during authorization as well.

Deployment Concepts

AUTHENTICATION SCHEME

AM Server - Authentication Module

The authentication framework of ForgeRock AM is based on the Java Authentication and Authorization Services (JAAS) framework. There are more than 20 authentication modules out of the box covering a large spectrum of technologies. You can also chain multiple authentication modules to provide multi-factor and/or step-up authentication as well to share state between each module. Risk-based and Fingerprinting authentication is also part of the standard product. Therefore, you do not need to purchase and install a separate component such as Oracle Adaptive Access Manager.

Deployment Concepts *Continued*

APPLICATION DOMAINS RESOURCES

AUTHENTICATION POLICY

AUTHORIZATION POLICY

CONSTRAINTS

RESPONSES

Realms/Policy SetsResource TypesAuthentication Chains/ TreesAuthorization Policy Sets
Oracle Application Domain: AM Policy Set DefinitionOracle Resources: AM Policy ResourcesOracle Response: AM Response AttributesOracle Policy: AM Policy DefinitionNote: AM provides a fine grain policy engine so the custom resource type and actions can also be defined. There is an opportunity for customer using Oracle Entitlements Server (OES) for Fine-Grained Authorizations to evaluate if they need OES or even if that capability can also be replaced by ForgeRock AM

DISTRIBUTED CREDENTIAL COLLECTOR

Identity Gateway (IG)
IG can act as an intelligent reverse proxy server between clients and the OpenAM Service. When deployed within a DMZ, OpenIG can inspect all traffic and properly forward requests to OpenAM.

Architecture

In any migration it is important to first understand the architectural differences between the old and new platform. Typically, an Oracle Access Manager deployment, which is deployed for scale, comprises of many “nodes” of Web Logic servers. In particular, there is a significant amount of Access Servers in the mix. The number of servers increase as you add more features and applications. This is not only problematic in an on-premise solution, but in a cloud environment it can be cost prohibitive and technically challenging. A ForgeRock deployment is simpler because a single ForgeRock AM server is able to provide many of the features that multiple instances of Oracle Access Manager can barely scale to provide. With a modern scalable architecture, ForgeRock AM still maintains high performance. Since the software is lightweight and DevOps friendly, it can be deployed easily in the cloud or on prem or hybrid topology with little or no “hands on” maintenance.

Secondly, the same multi-tiered architecture that is applied for Oracle Access Manager can still be used for the ForgeRock platform. Both choices of using a reverse proxy and individual agents are also available.

t is unrealistic to assume that all applications will work with a reverse proxy approach. There are COTS and other applications that cannot be modified at all, but still need to benefit from single sign-on. Here, ForgeRock has a unique solution of using the ForgeRock Identity Gateway (IG) to perform secure password replay onto applications. If the applications require information in SAML assertions or OAuth 2.0 scopes, IG can be used as an abstraction layer in front of your applications and pass information to them in any shape or form to be easily consumed, such as secure HTTP headers or even an API call.

The diagram below illustrates a typical migration topology. On the right are some of ForgeRock’s additional modern features are illustrated that are e available with the ForgeRock Identity Platform, including the tools provided to facilitate a migration. This is not a comprehensive list but identifies features pertinent to a migration.

In the below diagram, the OAM WebGate is shown on the container, but it can also be deployed on a reverse proxy. During the coexistence and migration, the OAM WebGate will be replaced with an AM agent, or optionally, the application can be fronted with IG as a reverse proxy and a smart gateway. The term "smart" refers to the fact that IG is not just a reverse proxy but has many features that allow it to route, map, transform, message, and replay requests to downstream systems such as your applications and other gateways. As an example, a "smart" role that IG plays is to act as a middleman for session keep alives so that as long as the session is active in one environment, it can be used to keep the other session alive. Similarly, if a session is destroyed in one environment, IG can terminate it in the other. This session "watchdog" role does require all requests to either of the environments pass through IG as depicted in the diagram.

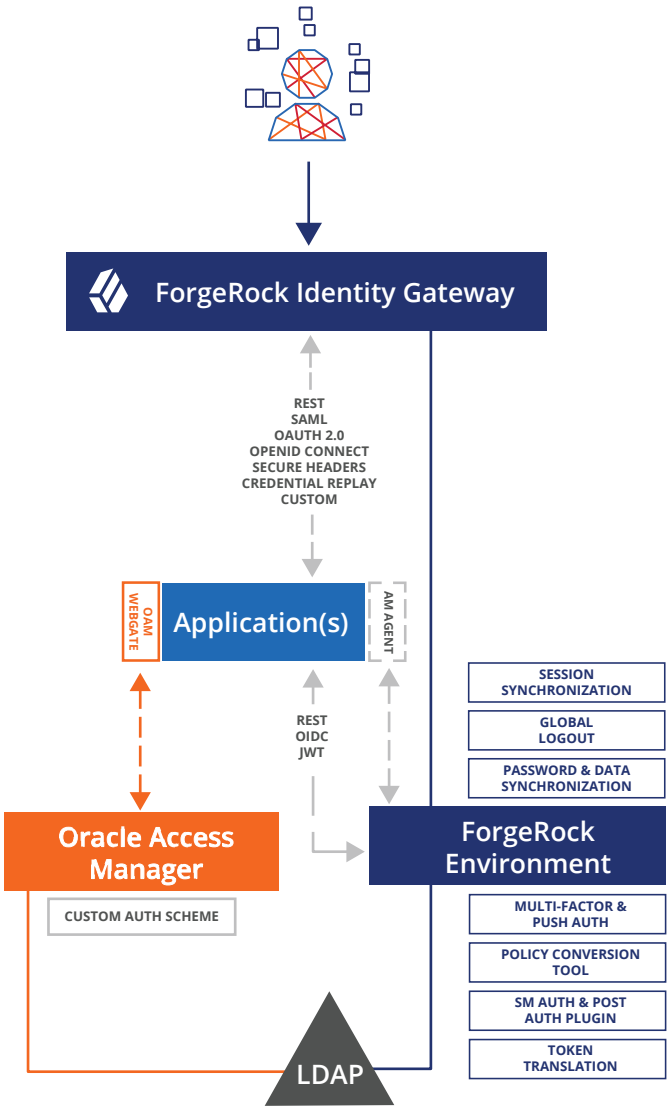

Diagram 2: Example of Migration Topology

Note the use of IG is optional and will depend on your migration strategy and business requirements.

Single sign-on between the two environments is facilitated by plugins provided by ForgeRock. A request with a valid Oracle Access Manager session to the ForgeRock environment will result in an automatic ForgeRock session creation. Conversely, if the request comes to the ForgeRock environment first, a post authentication plugin will create an Oracle Access Manager session using a custom Authentication Scheme provided by ForgeRock. This Authentication Scheme uses the standard interfaces provided by Oracle. Hence, the ForgeRock provided plugins ensure seamless single sign-on between the two environments. In fact, the end user doesn't really know which environment they are in. The key, however, is that the same identity repository is utilized for both environments. If, for some reason, separation of the identity repository is required, then the two disparate repositories should be synchronized during the coexistence phase. This synchronization can be bidirectionally automated with ForgeRock IDM. Alternatively, the "just in time" provisioning capability of AM can be utilized for first time logins resulting in a corresponding profile creation in the new repository.

Details

As mentioned earlier, the migration path is dependent on the complexity of your implementation of Oracle Access Manager, but in general the methodology is split into the phases shown in the diagram below. You can also combine some phases together if your deployment is simpler or if your deployment schedule is aggressive.

Phase 1: Plan

This is the most critical phase as careful planning will avoid unforeseen issues later. The key is to set realistic targets and timeline and to not try to "boil the ocean". If you have good documentation of your current environment, it makes this phase much easier to execute. Otherwise, as a first step, it is recommended to document your current deployment.

You should inventory the applications that are part of the Oracle Access Manager ecosystem, the relevant policies, and how each is utilizing current services. What type of authentication is it using? Does it have a WebGate deployed? What policies (if any) are associated with it? Is it using any API's? Are there any custom authentication plugins? What headers does it require, etc.?

The inventory should also identify the applications that are capable of being migrated to the new environment without any modifications, need slight tweaking, require modifications, or cannot be modified at all. Keep in mind that you don't need to touch your existing environment if you plan to first bring your new applications into the ForgeRock ecosystem, such as customer facing (CIAM) use cases.

The inventory will be used to define the application migration process and allow you to group them into "waves" of migration. Each wave can contain applications of different complexity and should be based on business requirements and compelling events. To help plan, some of the common migration challenges are listed below, along with pointers on how to resolve them.

Area	Use Case	How
Authentication (AuthN)	SSO from Oracle to AM SSO from AM to Oracle	› Use an authentication module for ForgeRock AM to validate OAM Session and then create an AM session › Use the Post Authentication Plugin for AM to invoke a OAM Custom Authentication Scheme and create an OAM session › Use the IG Password Replay via Form POST or Basic Auth
	Idle & Session timeout Global Logout	› Create a custom session "keep alive" filter on IG › Use a global logout filter on IG › Depending on your deployment, these can also be implemented without using IG, but will require custom coding and possible modification to your application.
Password Management	Passwords Account Lockout Warning Account Lockout Password Strength Password Retry Password History Self Service Password Reset (SSPR)	› You can migrate any standards password hashes directly into ForgeRock's DJ Directory. A large list of hashes are supported. In a worst case scenario, custom hashing algorithms can be added. › Password strength and policies can be matched › SSPR and Registration are OOTB features
Authorization (AuthZ)	WebGate Compatibility	› WebGate compatibility is not available. However, ForgeRock AM agents can provide the same or better functionality as the OAM WebGates. For example, AM provides far more agents, such as Nginx and various J2EE containers. Additionally, there is a community-supported agent for node. js. Another feature example is support for standards-based tokens such as OpenID Connect (OIDC) and OIDC Relying Party. › The two agents can also co-exist under certain constraints
	Policy Migration	› T his can be done via the policy migration tool provided by ForgeRock
STS	Token Translation Impersonation	› Via STS plugin that takes SMSESSION token and translates to ForgeRock Access Management SESSION token and vice versa
Federation	SAML	› Metadata and certificates can be exported and imported into AM
Customizations	3rd Party Customizations	› This is a case by case basis determination

Phase 2: Build & Co-Exist

First and foremost, in Phase 2, you stand up a ForgeRock environment for development and then QA. ForgeRock recommends standing up its environment using DevOps support in the platform, which allows you to maintain configurations as an artifact. Configurations can be checked into Git or any other version control system. If you use Git, then you can also integrate with JIRA to make this process automated. This way you can deploy the platform in any new environment with a hands off approach, minimizing human error and speeding up the deployment and recovery process.

Phase 2 is the phase where you become familiar with the ForgeRock Identity Platform. It is highly recommended to undergo ForgeRock training before this phase.

You should plan a pre-production environment in Phase 2 that can be switched to production mode later on.

Any new application can be added in Phase 2. In fact, most customers prefer adding at least one new application before migrating an older one. This helps ensure that urgent business needs that are identified during Phase 1 are completed.

Finally, in Phase 2 you should perform tuning and basic load testing of the ForgeRock environment to ensure that the impact of variables added in later phases can be measured and corrected if needed.

Phase 3: Migrate in Waves

In Phase 3 you migrate the applications identified in Phase 1 wave by wave.

Migrate your existing policies and other data into the ForgeRock environment using automated tools provided by ForgeRock. For example, the policy migration tool takes as input the dump of policies in xml and then creates a XACML3 file that can be loaded into AM directly.

ForgeRock AM does not require the use of its own user store and can be pointed to an existing LDAP v3 compliant user store. In Phase 3 you also configure ForgeRock AM to work with your existing user store so that there is no need to synchronize users between the two environments.

Migrate existing applications which are protected with OAM WebGates to be protected by ForgeRock agents.

Configure ForgeRock AM with the items identified in the planning phase (1) and with additional features and services that could not be provided in the legacy environment.

Phase 4: Decommission

Verify that there is no traffic coming to the OAM environment.

Remove all OAM WebGates from their respective containers.

Conclusion

This paper has presented details on how to co-exist and migrate from Oracle Access Manager to ForgeRock. These details are based on real life experiences, feedback from ForgeRock partners and customers and tests conducted in ForgeRock labs. There will be edge cases that are not covered in this document, but can be addressed in consultation with ForgeRock and its accredited partners. In summary, a carefully executed migration from Oracle Access Manager to the ForgeRock platform can not only be seamless, but will enable, transform, and catapult your business to the next generation of Digital Identity Services for your customers, employees and partners.

Meet Your Business Demands Today and Tomorrow with the Proven Visionary Leader

ForgeRock offers the most complete identity platform, the most powerful orchestration engine, and the best deployment options, including bring-your-own-cloud, hybrid-cloud, and multi-cloud models for millions of identities in minutes. Organizations adopt the ForgeRock Identity Platform™ as their digital identity system of record to monetize customer relationships, address regulations for privacy and consent (GDPR, HIPAA, PSD2, Open Banking, etc), and leverage the IoT.

As the leading visionary, ForgeRock defines the future of identity. Our mission is to provide the most simple and comprehensive Identity and Access Management Solution to help our customers deepen their relationships with their consumers, and improve the productivity and connectivity of their employees and partners. With ForgeRock, customers grow business and competitive advantage, increase productivity, improve security and compliance, and reduce costs