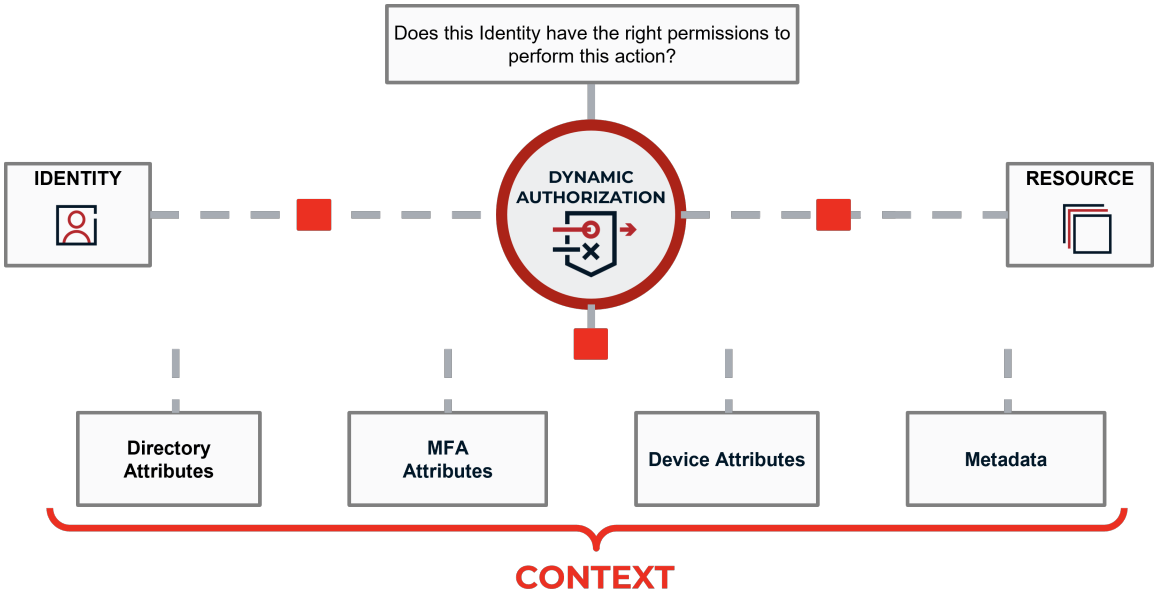
Attribute-Based Access Control

Attribute-based access control (ABAC) is a flexible approach to enable fine-grained authorization decisions for a requester (end entity/user) and a targeted resource/data/object. Each requester and resource has a set of associated attributes. These could include persistent attributes stored within a directory or contextual attributes such as time of request, type of multi-factor authenticator, device information, etc.

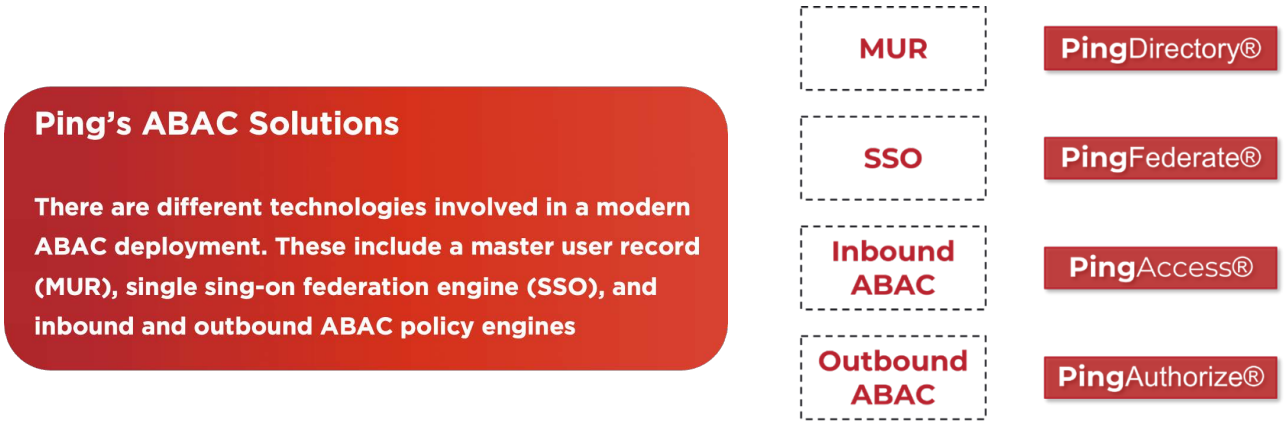


Historically, authorization decisions were based around RBAC or role-based access control. RBAC typically examines group membership, organizational position, and specific levels of admin rights or entitlements for determining access. While the attributes associated with RBAC decisions can be valuable for an organization, they are often too narrow in scope to account for the modern threat landscape.

"When authorizing users to access resources, agencies must consider at least one device-level signal alongside identity information about the authenticated user"
-OMB M-22-09

The Office of Management and Budget in their Federal Zero Trust Strategy memorandum (OMB M-22-09) calls for agencies to adopt the more granular-based controls found within ABAC for authorization decisions.

Ping Identity provides several products that can work together to enable and enforce ABAC. These products can be deployed independently, or in combination, as they are built around open-standards technology. This allows organizations to leverage the components necessary to augment existing investments to enable identity credential and access management (ICAM) modernization. These controls can be leveraged across an organiza-tion's footprint, including mobile, desktop, and web applications, and can be enforced through standards-based federation protocols, including SAML and OIDC, through header-based URL controls, and within the API layer.



Master User Record: PingDirectory

PingDirectory is a fast, scalable directory used to store identity and rich profile data. Organizations that need maximum uptime for millions of identities use **Ping**Directory to securely store and manage sensitive customer, partner, and employee data. **Ping**Directory acts as a single source of identity truth, and can be leveraged to create a Master User Record, or MUR, to store an aggregate of attributes for users, which can be used as an authoritative source of truth for supporting ABAC authorization decisions.

Having a MUR is an essential foundation for ABAC as it allows more holistic views and lifecycle management of users across an organization. The MUR is the logical integration point for identity governance and administration (IGA) engines, for quickly managing entitlements of users, as well as centralized policies for onboarding and offboarding.

Users get loaded into **Ping**Directory through import, API connection, manual entry or bidirectional, real-time synchronization from LDAP, RDBMS, JDBC, or SCIM data stores. Both structured and unstructured user data are secured and stored by leveraging encryption, password validators, cryptographic log signing, and more. **Ping**Directory helps organizations eliminate identity silos, and can become the authoritative record to be used for authorization decisions across the enterprise.

Single Sign-On: PingFederate

PingFederate is an enterprise federation server that enables user authentication and single sign-on. **Ping**Federate easily integrates with applications across the enterprise, third-party authentication sources, diverse user directories, and existing ICAM systems, all while supporting current and past versions of identity standards.

PingFederate can communicate and pull attributes from a diverse set of sources. These can include multiple directories and databases (including the MUR), external identity providers, and from the user directly through fields they input, and the credentials they present, during authentication. Additionally, its robust policy orchestration engine allows the integration of endpoint protection platforms (EPP) and extended detection and response (XDR), and other technology solutions into the adaptive authentication workflow to evaluate and enforce the device authentication prior to exposing user credentials.

These attributes can be passed to an authorization engine for ABAC decisions and enforcement.

Supported federation standards include OAuth, OpenID, OpenID Connect, SAML, WS-Federation, WS-Trust, and System for Cross-Domain Identity Management (SCIM). Additionally, PingFederate directly supports x.509 authenticators like the PIV and CAC, and can act as a federation hub to connect external identity providers into a centralized authentication policy engine.

Inbound ABAC: PingAccess

PingAccess is a centralized access security solution with a comprehensive authorization policy engine. It provides secure access to applications and APIs down to the URL level, and ensures only authorized users can access the resources they need. PingAccess allows organizations to protect web apps, APIs, and other resources using rules and other authentication criteria, and can be leveraged through agent-based and web access gateway-based deployments.

PingAccess enforces authorization by sitting between the user and the protected application. This enforcement is referred to as inbound ABAC, and it intercepts the requests between the user and the application and interjects a dynamic authorization decision to determine if the requesting user should have access to the requested resource within the application.

PingAccess enables and enforces course and medium-grained ABAC through its flexible authorization policy engine. The attributes examined by these policies can be pulled directly from assertions, tokens, and backchannel APIs sent from the federation engine, such as PingFederate, and/or from available directories, including the MUR. This allows PingAccess to augment the data provided from the federation engine with additional attributes available through configurable sources.

Outbound ABAC: PingAuthorize

PingAuthorize provides fine-grained access control using real-time context about users and the resources they are accessing to provide security and ensure compliance. It operates as a fine-grained authorization solution; leveraging real-time data to make authorization decisions for access to data, services, APIs, and other resources. PingAuthorize empowers administrators to set dynamic authorization policies to allow, block, filter or obfuscate an access request based on behavior, activity, or any other attribute.

PingAuthorize enforces authorization by sitting between the protected application and the data/resources being requested. This enforcement is referred to as outbound ABAC, and it intercepts the requests between the application and the data/resource being requested; typically handled by API requests. PingAuthorize builds in a dynamic authorization decision at this API level, and intercepts and modifies the requests based upon what the requesting user is authorized to access.

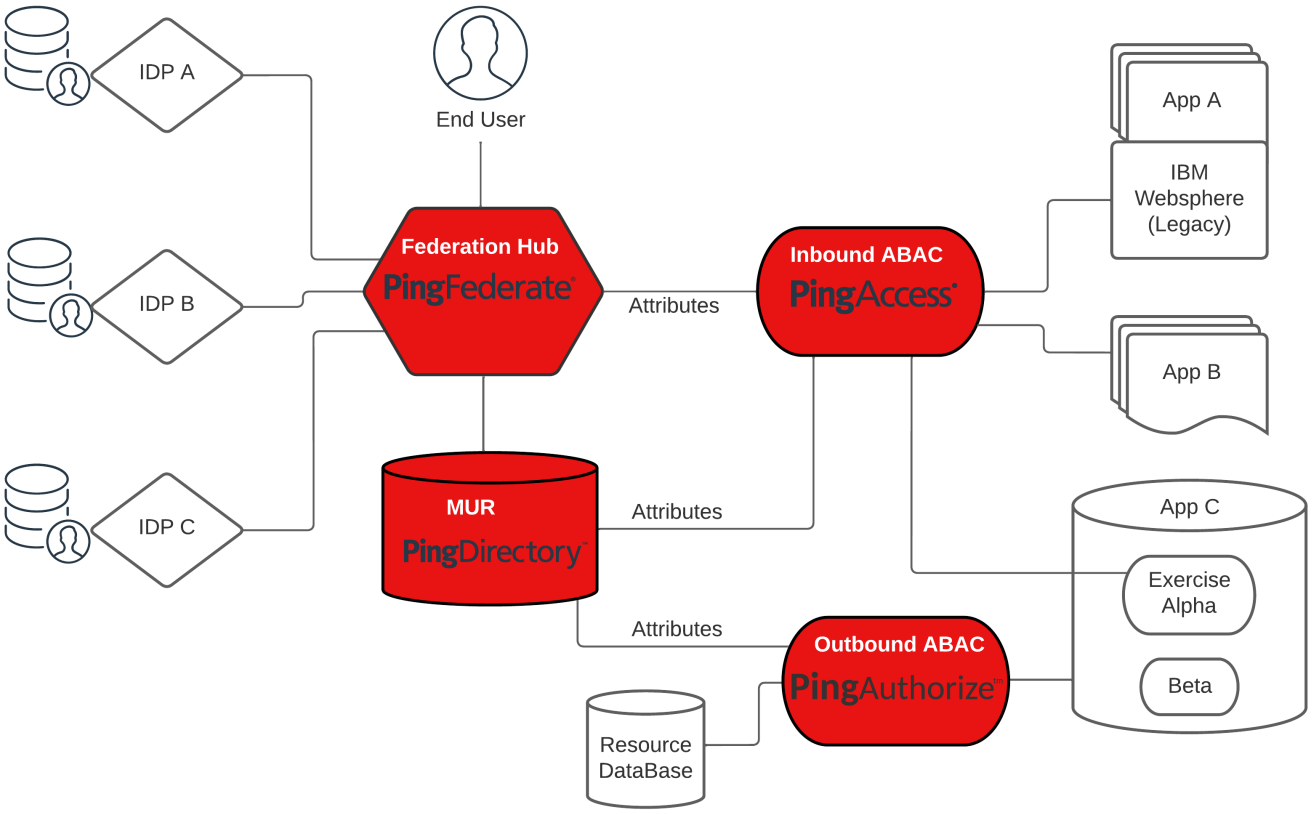
Dynamic authorization policies configured and enforced through PingAuthorize can evaluate any identity attribute, consent, entitlement, resource, or context to make ABAC decisions in real-time. PingAuthorize gives you centralized control over your digital transactions and application access to data.

Deployment Options

Every solution Ping Identity offers for US Federal customers can be deployed within Ping Identity's DOD IL5/FedRAMP High SaaS offering, in a private cloud, as a traditional application, and within air-gapped, DDIL, and/or network segmented environments, with full feature parity across all deployments. Each component can be administered through an easy-to-use graphical user interface, as well as through scripted and/or coded configurations through RESTful APIs.

Supported Deployment Methods:

- **FedRAMP High, DOD IL5 SaaS**
- **Private Cloud**
- **On-premises**
- **Hybrid (on-premises & cloud/hosted)**
- **DDIL**
- **Air-gapped, or network-segmented environments**



A Modernized ICAM built around ABAC

Ping Identity's unique portfolio allows external and internal identities to be centralized through a federation hub and master user record (MUR) with dynamic authorization through inbound and outbound attribute-based access control (ABAC)

For more information, visit www.pingidenity.com/fedgov

Ping Identity enables federal entities' distributed workforces to perform secure, interoperable mission-critical work from anywhere. We do this by providing the ICAM solutions and services organizations need to modernize their complex, hybrid envrionments and facilitate the move to a Zero Trust architecture.