The only enhanced AD/Entra ID connector for IGA

Introduction

Due to the ubiquity of Windows systems in enterprise environments, Active Directory (AD) is the most common enterprise identity management tool. However, integrating identity management across an organization's entire IT environment and implementing identity and access management (IAM) policies and best practices requires identity governance and administration (IGA) solutions.

Many organizations looking to connect these two processes face significant roadblocks, both at the technical and operational level. The Enhanced Active Directory Governance (EADG) Connector from One Identity simplifies this process by offering out-of-the-box integration between IGA and Active Roles for AD and Entra ID management.

The AD-IGA integration challenge

Connecting to AD is typically one of the first steps in an enterprise IGA deployment process. After integrating IGA with AD and a few other systems as a proof of concept, companies can work to integrate it with other systems.

However, setting up this initial integration can be complex. Some of the most common challenges that teams face include:

- **Security and protection concerns:** IGA and AD solutions need to share sensitive data, and misconfigurations of either, or a misalignment of the link between them, could expose the organization to data breaches or other security risks.

Abstract

Microsoft Active Directory (AD) and Entra ID remain the cornerstone of enterprise identity management, making them critical integration points for identity governance and administration (IGA) solutions. However, traditional IGA-to-AD integrations often present significant challenges around security, implementation and administrative delegation between IGA and AD teams.

The One Identity Enhanced Active Directory Governance (EADG) Connector revolutionizes this integration by combining the capabilities of One Identity Manager with Active Roles. Acting as a "super connector," EADG creates a secure proxy layer between IGA and AD/Entra ID that enforces policy controls, enables delegated administration and extends management capabilities beyond basic user and group operations—all while streamlining implementation.

The EADG Connector addresses key enterprise challenges by providing an AD and Entra ID "firewall" that protects against misconfigurations, enabling AD teams to manage workflows using familiar tools without learning complex IGA interfaces. It also extends object management to include mailboxes, devices and virtual attributes without schema modifications. This unique approach significantly reduces implementation time and complexity while enhancing security and governance capabilities, particularly in complex multi-forest environments.

- **Team delegation complexities:** AD and IGA teams have overlapping responsibilities but, potentially, competing goals, creating tension and complicating task delegation.
- **Implementation hurdles:** When implementing IGA, teams commonly struggle to master new IGA tools, connect solutions to complex AD environments and define and enforce consistent policies.
- **Schema extension limitations:** Extending an AD schema comes with risks, such as the inability to revert permanent schema changes and the potential that some applications may not be compatible with the extended schema.
- **Multi-forest management issues:** Consistent policy enforcement, identity synchronization and attack surface management grow more difficult as additional domains and forests are introduced.

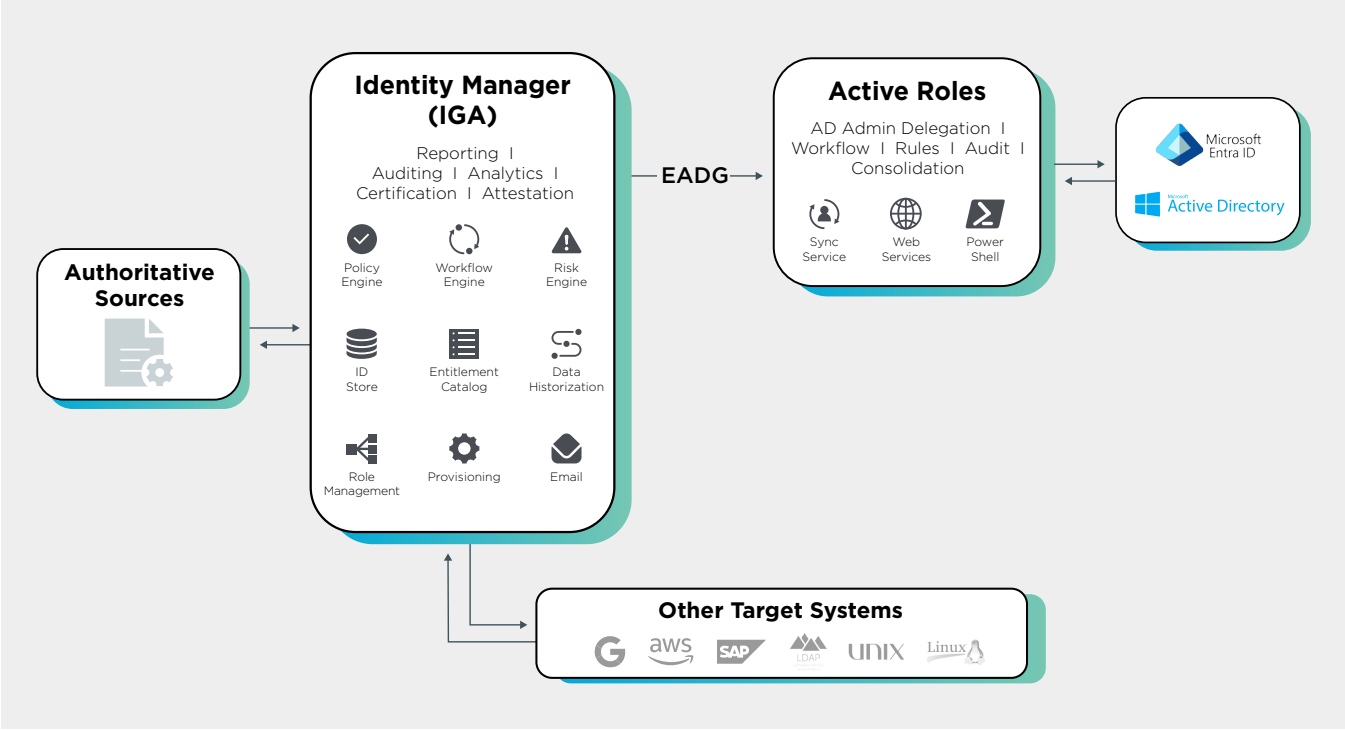
EADG Solution Architecture

Can we simplify this paragraph? For example: EADG from One Identity provides a connector between Identity Manager (IGA) and Active Roles, which integrates directly with AD and Entra ID and provides the following capabilities:

1. Automation of workflows for streamlined AD administration
2. Fine grained delegation for accounts and groups
3. Change tracking for simplified auditing
4. Cleansing of directories for ease of migration

The One Identity EADG solution architecture includes the following components:

- **Identity Manager:** Identity Manager connects to authoritative sources and provides centralized identity monitoring and management.
- **EADG Connector:** EADG bridges the gap between Identity Manager and Active Roles, linking traditional IGA with an AD or Entra ID environment.
- **Active Roles:** Active Roles is responsible for managing an organization's AD and/or Entra ID deployment, streamlining operations and enhancing security.



Key Features & Benefits

EADG is a "super connector" that goes above and beyond the capabilities and benefits of a standard IGA AD or Entra ID connector. Some of the key features that it provides include:

- **AD/Entra ID protection:** EADG implements a "firewall" for AD/Entra ID, enabling policy-based protection against misconfigurations and security gaps.
- **Delegated administration:** EADG simplifies IGA administration by allowing AD/Entra ID teams to manage their IGA via their native tools and workflows without the need to learn a new IGA tool.
- **Extended object management:** With EADG, teams can manage not only users and groups, but mailboxes, devices and virtual attributes without the need to perform modifications to AD schemas.
- **Simplified multi-forest support:** Multiple domains and forests can be managed within a single IGA instance using EADG, simplifying identity management across the organization.
- **Implementation acceleration:** The pre-built connector in EADG streamlines IGA deployments, minimizing the scope and risk of an enterprise-wide deployment and reducing time to value.

Use cases

One Identity EADG is the only pre-existing connector for IGA and AD. This lends itself to various use cases, including the following:

- **Enterprise AD security:** EADG offers native protection against common AD security risks, such as misconfigurations and overprovisioning. Policy-based protection against mistakes and malicious actions reduces the risk of breaches and simplifies regulatory compliance.
- **Complex AD environment management:** EADG allows an IGA team to quickly and easily integrate their solution with multiple AD domains/forests. With EADG, organizations can more consistently enforce security policies and protect complex AD environments against attack.
- **Team collaboration:** AD and IGA teams may have conflicting priorities and lack desire to learn new tools and processes. With EADG, the AD team can continue working with familiar tools and workflows built for them, reducing potential friction.
- **Migration and implementation:** With a prebuilt connector for AD and IGA solutions through EADG, organizations can implement IGA or perform a migration more easily than if all configurations were performed using automation.
- **Compliance and governance:** EADG provides superior visibility and control of critical identity attributes and objects at a central location. By enabling policy-based management and eliminating visibility gaps, it simplifies the process of achieving and demonstrating compliance with applicable regulations.

Business value

The EADG connector from One Identity offers a secure, option for IGA-AD integration. Some key business benefits it provides include:

- **Cost reduction:** EADG is the only prebuilt connector for IGA and AD and offers various features to streamline AD management and to enhance the security of AD deployments, protecting against costly data breaches and other incidents.
- **Risk mitigation:** EADG addresses various potential sources of risk to the business by offering policy-based protection against misconfigurations and other common AD security risks.
- **Team efficiency:** EADG makes it easy to define roles for IGA and AD teams and enables them to use the tools and workflows that they prefer, enhancing their efficiency.
- **Implementation speed:** EADG accelerates IGA implementation by eliminating manual efforts to connect IGA and AD or Entra ID, a common roadblock that teams face in the IGA deployment process.
- **Total cost of ownership (TCO):** EADG reduces TCO by decreasing the deployment time for IGA and offering streamlined workflows to enhance business efficiency.

Conclusion

IGA-AD integration is a common challenge for many companies due to competing team priorities and a lack of simple integration solutions. The EADG Connector from One Identity simplifies IGA-AD integration and management while enhancing the security of a corporate AD deployment.

Learn more about EADG and its potential benefits for your organization in the EADG connector solution guide.

About One Identity

One Identity helps organizations strengthen cybersecurity, boost efficiency and control costs through the One Identity Fabric, a holistic approach to identity and access management (IAM). By unifying IAM tools, including identity governance and administration (IGA), access management (AM), privileged access management (PAM), and Active Directory management (AD Mgmt), it ensures optimal functionality and efficiency. This cohesive structure reduces identity sprawl and extends governance to the farthest endpoints of your IAM ecosystem. Proven and trusted on a global scale, One Identity manages more than 500 million identities for more than 11,000 organizations worldwide. For more information, visit www.oneidentity.com.

ONE IDENTITY