clarity

2024 GUIDE

Navigating Identity Governance with a Complex AD Infrastructure

How to Overcome the Common Obstacles and Build a Successful Identity Governance Program Within Your Hybrid AD Environment

Table of Contents

clarity

Introduction

When it comes to building successful identity governance programs, hybrid environments can present some unique challenges. While some of the most prominent voices in the IT security space are advocating to remedy this by adopting fully cloud-based environments, that shift simply isn't feasible for many leaders who rely on the benefits a hybrid system provides as the foundation of many of their existing IT ecosystems.

So, what's the alternative?

This guide is built for security leaders with hybrid AD environments who are currently looking to build successful identity governance programs. In it, we will cover:

- The benefits of maintaining a hybrid AD environment
- An overview of the current IGA solutions available, and what they offer to help those with complex environments
- What IT leaders with complex AD environments should be doing to properly vet an IGA vendor
- The impact of multi-domain AD environments on an organizations IGA efforts (and goals)
- The process for manually tackling user access reviews in a complex AD environment
- How Clarity helps

AD Environments

First, let's review the two AD options offered by Microsoft.

Microsoft Active Directory (AD) and Azure Entra, formerly known as Azure Active Directory (Azure AD), are both directory services provided by Microsoft. However, each serves different purposes. Here are the main differences between them:

	Hosting	Scope	Governance
Active Directory	On-premises	• Manages users, groups, computers, federated access, and other resources within a Windows environment. • Provides Group Policy Objects for granular control over user and computer.	• Relies on traditional security measures within an on-premises network. • Uses Security Groups and Group Policies for governance and control.
Azure EntraID	Cloud	• Manages identities for users, groups, and applications in the cloud. • Provides Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Conditional Access policies.	• Enhanced security features such as Identity Protection, Privileged Identity Management (PIM), and access reviews. • Advanced monitoring and reporting capabilities for cloud identities.
Hybrid	On-Premises + Cloud	Azure AD Connect is a tool used to synchronize on-premises AD objects to Azure Entra, enabling a unified identity for users across both environments.	

Why would you stay in a hybrid environment?

By maintaining a hybrid environment, companies can achieve a balance between leveraging modern cloud capabilities and maintaining control and security of their existing on-premises infrastructure. This approach provides a flexible, scalable, and compliant solution that meets diverse organizational needs.

Legacy Systems and Applications

- Many organizations still rely on legacy systems and applications that require on-premises Active Directory for authentication and management, performance requirements, or compliance requirements that mandate on-premises infrastructure
- Migrating these systems to the cloud can be complex, time-consuming, and costly.

Control Over Cost/Transition to Cloud

- A hybrid environment provides a gradual transition path to the cloud, allowing organizations to move workloads and applications at their own pace.
- Maintaining a hybrid environment allows organizations to balance costs between on-premises infrastructure and cloud services.
- This approach reduces the risk and disruption associated with a full-scale migration.

Data Sovereignty and Residency

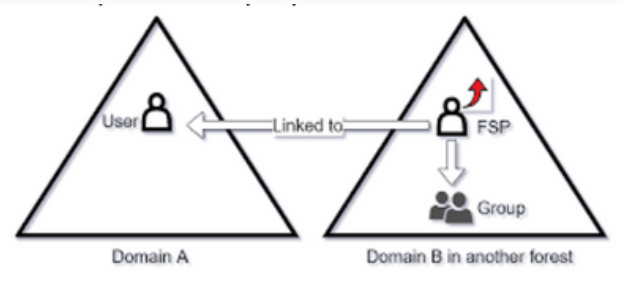
- Some organizations need to keep certain data within specific geographical boundaries due to legal or policy requirements.
- On-premises AD ensures that sensitive data remains within the organization's control, while Azure Entra can handle less sensitive, cloud-optimized workloads.

Governance Risks for Hybrid AD Environments

Hybrid AD environments bring extra complexity to IGA efforts. Most organizations that use on-premises AD have a reliance on capabilities that are not found in Entra ID, including the ability to have federated access between multiple domains and home-grown applications.

As your Domain Admins might tell you, LDAP queries do not return the full scope of a user's access if the user also has foreign security principals in a multi-domain forest. Similarly, if a Security Group is a foreign security principal and is a member of Domain Admins, this access will be missed. The problem is self evident. It rapidly creates over-provisioned nested access, alack of complete visibility to who has access to what, and requires manual inspection of AD hierarchy to inspect what access is granted, which isn't feasible for AD forests with more than 100 users.

For example, if a group (or nested group) grants sensitive access through a FSP (like the diagram below), it's not possible to query that nested access on Domain A.



So what kinds of risks does this issue create?

- Not reviewing the full access of employees/contractors in the organization during audits
  - This is VERY possible with nested groups and trust relationships. Native AD tools and most IGA vendors don't handle this. If your company has had any M&A or a corporate rebrand or just has complex AD infrastructure, this has to be handled manually.
- Over-provisioning access and not following least privilege principles
  - Same issue, if you don't review the nested group hierarchy regularly, extra access will always be created. Humans are not great at understanding the deeper implications of group changes which are never immediately obvious from a business/risk impact perspective
- Creating unexpected/risky access
  - Group nesting can lead to granting sensitive access to many more people than expected, especially when AD is ALSO providing federated access to downstream applications. Group A -> Group B -> Federated Application C (changing group A membership has implications for Application C that are hidden and non-intuitive)

Common Key Capability Challenges

Support for Hybrid Environments

This is probably not a surprise, but not all vendors support on-premises AD or hybrid environments, or if they do support them, its with material limitations

Support for Multiple Domains

This is needed to handle marketing rebrands, acquisitions or other domain changes. This is VERY common, and an AD domain consolidation won't be on the priority list for your C-suite just because your IGA solution doesn't support multiple domains.

Support for Nested Entitlements

If you have on-premises AD, you likely have nested entitlements. EntraID's limitations around nested entitlements makes it a very manual process to try to use Microsoft's native access review tool, but it's key to a full access review. Don't be caught out by your auditors.

Support for Role Based Access Control (RBAC)

Microsoft doesn't support RBAC in hybrid environments, but RBAC is best practice, this causes major friction for IT organizations

Support for Foreign Security Principals (FSPs)

If you have on-premises AD, you likely have nested entitlements. EntraID's limitations around nested entitlements makes it a very manual process to try to use Microsoft's native access review tool, but it's key to a full access review. Don't be caught out by your auditors.

What IGA Solutions Can Support AD and Hybrid AD Environments?

	SailPoint	Saviynt	Okta	Pathlock	FastPath	MSFT	Clarity
Active Directory	X		Agent			X	X
EntraID	X	X	X	X	X	X	X
Hybrid AD	X					X	
Nested Groups Hierarchy	X					X	X
Nested Groups Access Reviews							X
Multi-Domain			Partial			X	X
Foreign Security Principles							X
RBAC for Hybrid AD							X
Requires Universal Directory			X			X	

Key IGA Features for Hybrid AD Environments

RBAC for Hybrid AD Environments

Role Based Access Control is a security best practice that allows companies to simplify access management, improve compliance and auditing, and reduce their exposure to insider threats or mis-use of access. Unfortunately, Microsoft EntraID does not support RBAC in a hybrid AD environment, as AD groups can't be added to Entra Roles.

Resource:https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept

- **Simplified Access Management**
  - Managing access through roles makes it easier to assign, modify, and revoke access rights as users change roles within the organization.
  - RBAC is scalable and can accommodate the growth of an organization. Access permissions can be easily adjusted without having to update individual user accounts.
  - RBAC promotes consistency to ensure that security practices are uniformly applied and maintained.
  - New roles can be created, updated, and assigned as needed without overhauling the entire access control system.
  - Dynamic role assignment based on attributes or rules allows for automated adjustments to access rights as users' roles or attributes change.
- **Compliance and Auditing**
  - Many regulatory frameworks (e.g., GDPR, HIPAA, SOX) require strict access control measures. RBAC provides a clear, structured approach to access management.
  - RBAC enables comprehensive auditing of access permissions and user activities. It is easier to track who has access to what resources and when changes were made.

- **Minimized Risk of Insider Threats**
  - Least Privilege: RBAC ensures that users are granted the minimum level of access necessary to perform their job functions, reducing the risk of accidental or malicious misuse of sensitive information and systems. RBAC also reduces the number of potential entry points for attackers, thereby lowering the risk of breaches.
  - Separation of Duties: RBAC can enforce the separation of duties by ensuring that critical tasks are divided among different roles.

- **Reduced Administrative Overhead**
  - Onboarding/Offboarding: With RBAC and lifecycle management, onboarding new employees and offboarding departing ones is more efficient. New users can be quickly assigned to appropriate roles, and access can be promptly revoked when users leave the organization.
  - Delegated Administration: RBAC allows for delegated administration, where role management can be distributed to department managers or specific administrators, reducing the burden on central IT teams.

Multi-Domain Support + Foreign Security Principles

- High level: FSPs give admins the ability to grant AD access in Domain B to users/groups/group managed service accounts that only exist in domain A without actually creating a new user/group/gmsa.
- This tool is powerful because:
  - Users can keep their normal username and password to log into the apps associated with a newly acquired company.
  - Homegrown RBAC (also known as birthright or baseline access) using AD groups can be retained as you can grant current AD groups additional baseline access in the new AD domain.
  - And! It means your business critical apps do not need to be modified as their source/federated domain will not change! This means no downtime, no potential outages, and no risk of lost revenue.

Nested Groups and Access Reviews

Nested groups in the context of Active Directory (AD) and Azure Entra (formerly known as Azure Active Directory) refer to the practice of including one group as a member of another group. This concept can be used to simplify administration and provide granular control over access and permissions. Here is an overview of nested groups and their implications in both AD and Azure Entra:

Active Directory (AD)

- Benefits:
  - Simplified Administration:
    - By nesting groups, administrators can manage permissions and access more efficiently. For example, rather than assigning permissions to individual users, permissions and groups can be assigned to a parent Security Group.
    - Nested groups allow for a more organized and hierarchical structure
  - Scalability:
    - As organizations grow, nested groups provide a scalable way to manage access without having to manually update every user or flat group.
    - Existing groups with well-defined permissions can be reused within other groups, reducing redundancy and potential errors in permission assignments.
    - It's easy to incorporate additional domains (Ex. acquisition / rebrand)
- Challenges:
  - Complexity and Troubleshooting
    - The use of nested groups can add complexity to the directory structure, making it harder to understand and manage permissions, especially in large organizations.
    - Diagnosing access issues can be more challenging when permissions are inherited through multiple nested groups.

Both Active Directory and Entra ID are Microsoft products, and they've had years to decades to resolve these differences in functionality. It's quite likely these limitations are forever.

The promise of Entra ID is that it will completely replace Active Directory for customers, and provide all the same functionality for complex enterprises. The reality is far from that, and that hybrid environments are the de facto standard due to Entra's limitations. One of the larger issues is the inability of EntraID to manage AD groups directly, forcing companies to completely migrate the group management to Entra, an impossible task for some organizations.

Note:https://learn.microsoft.com/en-us/entra/identity/users/directory-service-limits-restrictions

How Can I Perform Access Reviews Without a Third-Party Solution?

It's always helpful to understand what it would take to do it yourself, then you can assess if it makes sense to invest in a 3rd party solution. Here's a guide on how to create your own process.

Step 1: Determine which groups and resources need to be reviewed.

Step 2: Collect Group Membership Information

Extract On-Premises AD Group Information (repeat this for each domain)

- Use PowerShell to export group memberships, including nested groups, from on-premises AD.

```
Unset
Get-ADGroupMember -Identity "GroupName" -Recursive | Export-Csv -Path "OnPremGroupMembers.csv"
```

Extract Azure Entra Group Information

- Use Azure AD PowerShell or Microsoft Graph API to export group memberships from Azure Entra.

```
Unset
Get-AzureADGroupMember -ObjectId "GroupObjectId" -All $true | Export-Csv -Path "AzureADGroupMembers.csv"
```

Step 3: Analyze and Flatten Nested Groups.

Flatten Nested Group Structures

- Use scripts or tools to recursively resolve nested groups and produce a flattened list of users for each group.

```
Unset
Function Get-NestedGroupMembers {
  Param (
    [Parameter(Mandatory=$true)][string]$GroupName
  )
  $members = Get-ADGroupMember -Identity $GroupName -Recursive
  $members | ForEach-Object {
    if ($_.objectClass -eq "group") {
      Get-NestedGroupMembers -GroupName $_.SamAccountName
    } else {
      $_
    }
  }
}

$allMembers = Get-NestedGroupMembers -GroupName "GroupName"
$allMembers | Export-Csv -Path "FlattenedGroupMembers.csv"
```

Consolidate Data

- Combine the flattened membership data from on-premises AD and Azure Entra into a single dataset for analysis.
  - Note: This requires extensive ETL experience with excel

Step 4: Conduct Access Review

- Take the CSV data and work to assign the review to relevant owners who can make good decisions about the access (likely AD administrators or application owners)
- Check each user's membership and ensure it aligns with their job roles and responsibilities.
- Look for any discrepancies or unauthorized memberships.

Step 5: Implement Changes / Remediate

Remove Unnecessary Access

- Based on the review findings, remove users who no longer require access.
- Update group memberships accordingly in both on-premises AD and Azure Entra.

Document Changes

- Keep a record of the changes made during the access review for auditing and compliance purposes.

Step 6: Schedule Regular Reviews

- Set up recurring reviews to ensure continuous compliance. (this requires completing all the prior steps before each review)
- Continuously monitor group memberships and access rights.
- Use SIEM solutions to audit changes and detect any anomalies in real-time.

By following these steps, you can effectively conduct manual access reviews for nested groups in a hybrid AD environment, ensuring proper governance and security of your organization's resources.

What Can Clarity Security Do For You?

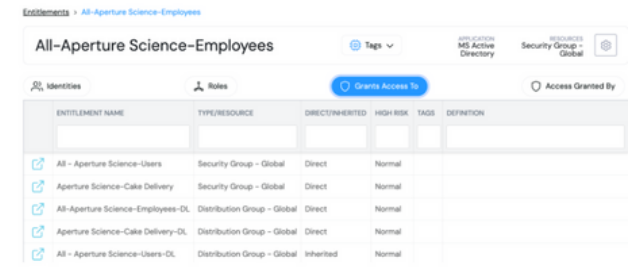
Clarity has invested heavily in support for complex Active Directory and Hybrid Entra ID environments. We have native support for the key capabilities that make running access reviews simple even in the most complex environments. This is part of our philosophy of “take things as they are”. We want to support your AD environment as it is, not require months of investment in change management, data cleanup or other efforts in order to execute your governance program.

Here’s what it looks like–

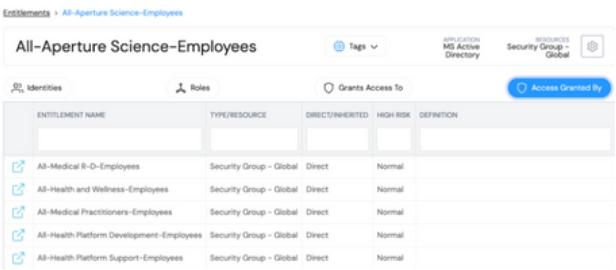
Clarity provides a native AD connector that supports BOTH multiple domains/forests, and nested groups. You connect Clarity to your AD forest(s), and we traverse the domains/trusts to identify all access. It’s a single connection, we sort out the rest.

Clarity will then enrich the data, linking the groups from one domain to another, and build the hierarchy of access showing both parents and children. The hierarchy will show the “correct” user friendly name, not the foreign security principal Id’s that Active Directory provides.

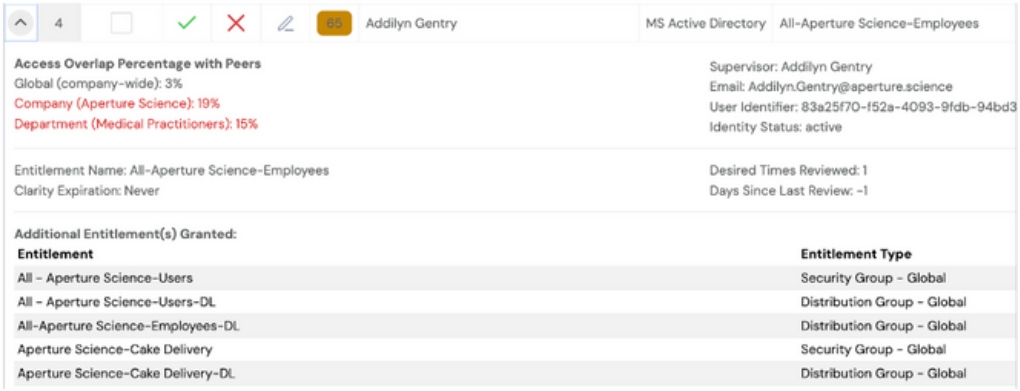
Example Parent Group List



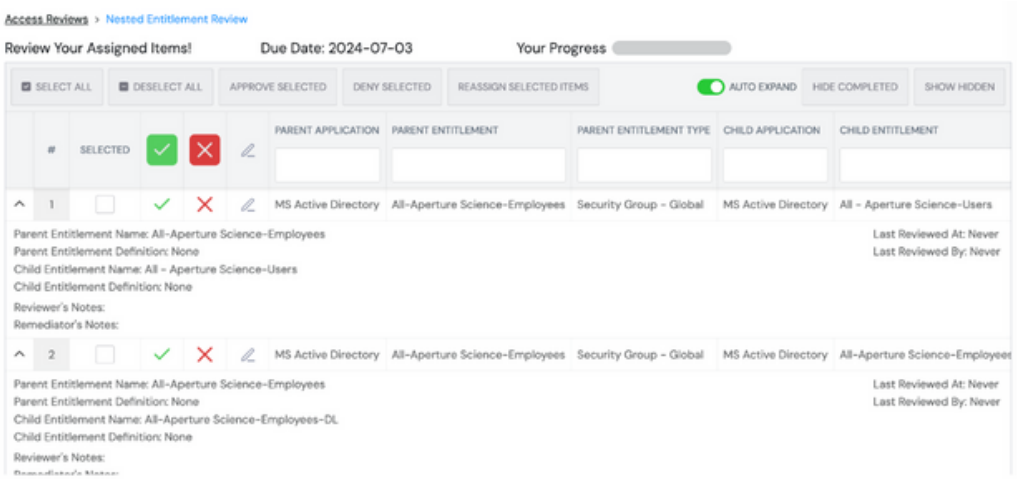
Example Child Group List



We then enrich user access reviews, showing the full access being approved within the review. This helps your managers and application owners spot if there is inappropriate access being provided as part of the group nesting.



You can also review the group hierarchy directly, which allows you to certify your group nesting is valid and appropriate. This kind of review is typically done by AD administrators.



Leveraging these capabilities is simple:

1. Connect to AD (one connection for all the environments - no extra preparation needed)
2. Tag key entitlements and downstream applications
3. Run your reviews as normal (Clarity already did the heavy lifting) but now enriched with all the nested group data
4. Add a new "nested group review" to your governance program to review the nesting and ensure nothing was added that isn't expected
5. Have a much more sustainable access review program for your central permissioning system, active directory.

Conclusion

There are many options for how to handle complex AD environments, but Clarity has developed the simplest to deploy, least effort solution to date.. This is an incredible boost to IT security teams challenged to mitigate identity risks being created by business drivers outside their control. In many cases, it's just not feasible to remove multiple domains, trusts, or nested groups from your AD environment. Existing solutions require un-sustainable manual work, or complex IT infrastructure overhauls, both of which are unacceptable. With Clarity's new capabilities, the promise of easy 10 minute access reviews is achievable, even for the most complex AD environments.

To learn more, please contact us at sales@claritysecurity.com or request a personalized demo of these capabilities at https://claritysecurity.com/request-a-demo.