



Access Control Is Easy

Use Active Directory groups and manage them well

Written by Randy Franklin Smith, president, Monterey Technology Group, Inc.

Introduction

Good access control requires managing most entitlements through Active Directory

Good access control is really a matter of well-managed groups. Of course, the why and how of access control matter, too, and I'll cover that in this solution brief. But at the end of the day, good access control comes down to avoiding the use of local groups (whether on Windows file servers, in Microsoft® SQL Server®, in SharePoint®, or elsewhere) and

instead assigning permissions to Active Directory® (AD) and Azure Active Directory (AAD) groups. In my experience, you can't hope to really understand, much less control, who has access to what until you can manage the bulk of your entitlements through AD.

In this paper, I'll explain why AD groups are at the center of the access control and governance universe and then explore what it takes to manage them. I will discuss why and how to implement group ownership and attestation controls. Also,

we'll look at how much group maintenance can be automated through self-service access-request handling and policy-based rule assignments.

You can extend access control to most applications and technologies.

Not every application can support such an AD-centric approach to group and entitlement management. Nor will every IT group agree to it. But that doesn't mean that you must give up the benefits of good

access governance. We will look at methods for extending your access-control framework to less integrated applications and technologies and managing AD securely in such environments.

Access control also requires managing administrative authority.

End-user entitlements aren't the only story in access control. It's important to control administrative authority—especially in AD. Also, given how crucial AD is as the center of enterprise access control, the manageability of AD becomes an important issue.

Good access governance means cataloging your resources, understanding the entitlements each user has and how appropriate they are relative to the user's role and peers, identifying the best person to make decisions about access to each resource, and then automating as much of that approval and periodic review process as possible. AD has

emerged as the best place for most organizations to hold this information.

In this brief, we'll look at how to manage AD for security and business efficiency. The One Identity family of identity and access management solutions is a leader in this area, and I think you'll be impressed by how Identity Manager helps you to implement this paper's recommendations on group and entitlement management. I'll also discuss how Active Roles can solve related critical issues with AD management and integration to improve overall security and governance. And Starling Identity Analytics & Risk Intelligence (IARI) provides the ability to assess risk relative to user permissions, rights, and entitlements and remediate issues.

Overview: the five commandments of access control

Implementing good governance in access control is a matter of


managing groups according to five best practices of entitlement. I will explain each of these five "commandments" and then discuss how they are applied to group management. I will highlight important caveats and challenges and show how Identity Manager and related products can help you implement the recommendations and address their inherent challenges.

One: Ensure central visibility of all entitlements.

The two key questions that you have to be able to answer

Access control is about two major questions that must be answered over and over again during the lifecycle of a user account, as well as during security and governance processes:

- What does user X have access to?
- Who has access to resource Y and why?



Access control is about two key questions: "What does user X have access to?" and "Who has access to resource Y and why?"

Active Roles protects AD from unauthorized and non-compliant changes.

Answering these questions in a timely fashion is crucial to effective governance, managing risk, and controlling costs. If an organization must search through many systems and resource access control lists every time one of these questions arises, then governance will suffer and security risk and operating costs will increase. The solution is to implement an access control structure that leverages the centric nature of AD so that these two questions can be answered from within AD alone.

All the other best practices in this paper will help you answer those two key questions.

The other “commandments” in this paper are building blocks to this purpose. For instance, one element of the next commandment prohibits the use of local groups in servers and applications. The organization that ignores this warning, uses local groups for entitlements, and

tries to determine what user X has access to must essentially search through every local group on every server and application to see whether the user is a member. But the organization that avoids local groups and follows the other recommendations in this paper needs only to look at the user’s group memberships in AD and the nested memberships of those groups. From there, that organization can list all the entitlements of the user—without ever leaving AD.

Two: Never be redundant.

Redundant groups lead to security issues and increased costs.

Redundancy is a universal gremlin in the IT world. The issue ranges from un-normalized relational databases to duplicated fragments of code in software. Redundancy—whether in the form of data, code or lists of people—causes problems: all these forms of information must be updated,

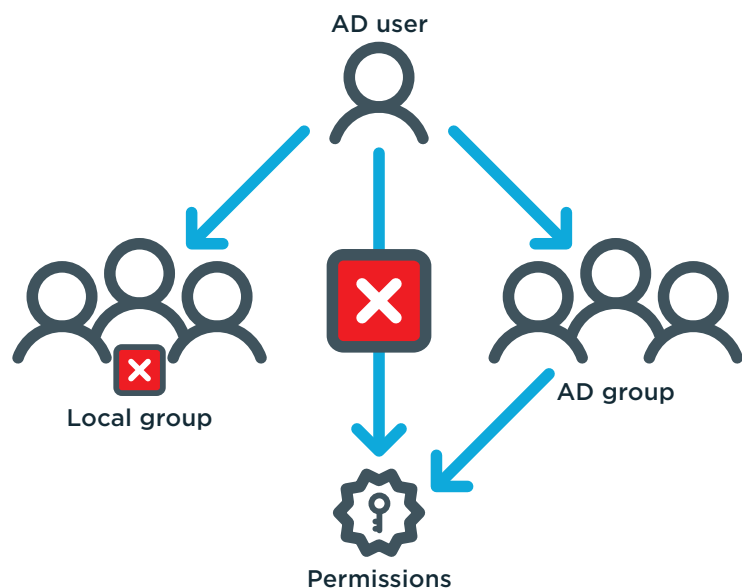


Figure 1. Use AD groups to manage access.

For systems and applications that cannot leverage AD groups, implement integration technologies to synchronize groups between AD and other systems.

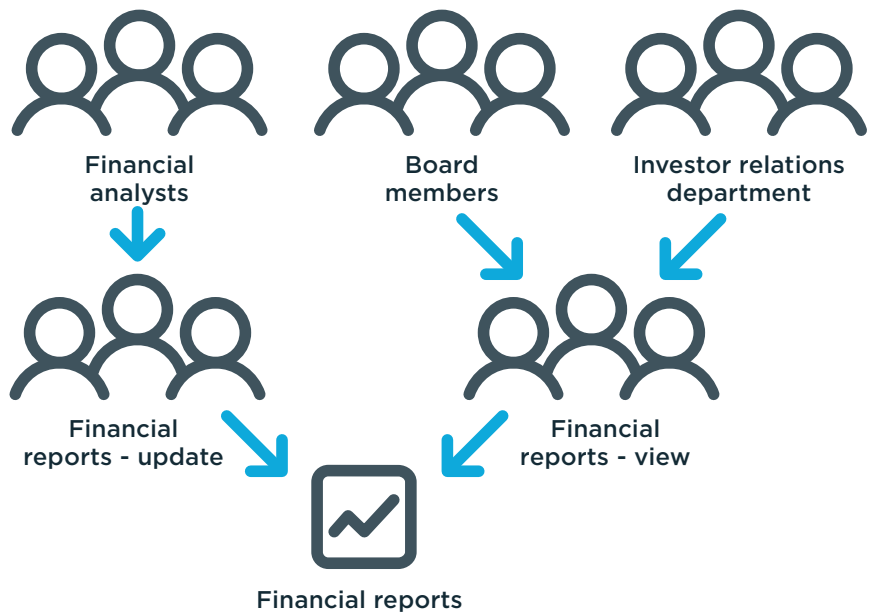


Figure 2. Use a two-level group structure to separate roles and entitlements.

and keeping multiple copies of the same information up to date is expensive and error-prone.

In access control, that translates to users with inappropriate access, as well as increased IT management costs as administrators hunt down entitlements and struggle with confusing group and permission structures.

There are two primary causes for redundant groups:

- Lack of basic management controls for groups
- Use of local groups on member servers and inside applications

Redundant groups can be caused by lack of basic management controls for groups.

In my consulting firm's IT audit practice, we frequently encounter

groups with very similar names and the same (or nearly the same) list of members. For instance, we might find a group called "Human Resources" and another named "HR Dept" with 90–100 percent duplicate members. Invariably, IT staff is hard-pressed to explain the difference in the groups in terms of entitlements, membership criteria, or differentiating purpose.

There is seldom a real answer because there never should have been two groups in the first place. But because of a lack of controls, past IT administrators were allowed to create groups without first checking for existing groups that met their purpose, or such information was simply unavailable. Administrators are often unsure of a group's purpose because it isn't documented anywhere and the original administrator who created the group is gone.

Your access control structure should reflect the business rules that drive it, yet remain flexible enough to securely handle the inevitable exceptions that arise.

Active Roles protects AD from unauthorized and non-compliant changes. It does so through a proxy service that allows administrators to complete their work faster than ever by implementing least-privilege and accountability at the same time.

Redundant groups can also be caused by use of local groups on member servers and inside applications.

Redundant groups also accumulate in an organization when, for expediency or due to lack of training, administrators create local groups instead of keeping all groups in AD. Windows member servers allow you to grant permission to AD domain groups or to local groups that are created in the local security database of that system. Likewise, most applications, such as SharePoint and SQL Server, support some type of local group. But the use of local groups¹

to control access to resources creates two problems for governance, security, and cost:

- **Redundant groups** — Invariably, a given set of users corresponding to some role, team, or responsibility in an organization needs to be granted access to resources on more than one server or application. Local groups are accessible only within the system or application on which they are created. Therefore, administrators of each application or system end up creating essentially the same group with the same users.
- **Lack of central visibility into entitlements** — The use of local groups results in entitlements being scattered throughout every system and application.

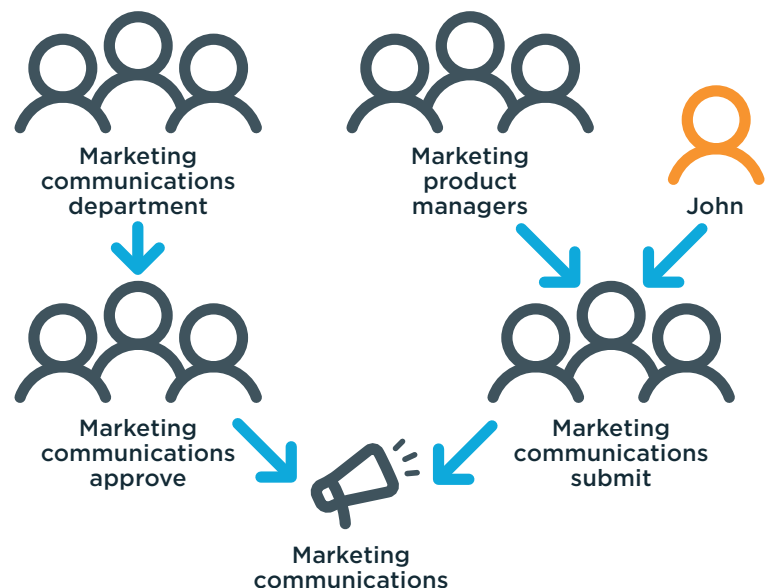


Figure 3. How to handle exceptions (like John) securely.

¹This statement does not apply to intrinsic local groups, such as the built-in Administrators group on Windows systems.

Eliminating redundancy

To eliminate redundancy, follow these guidelines:

- **Grant permissions to groups, not users.** It goes without saying that you must use groups in the first place. But I still find permissions granted to individual users instead of through groups.
- **Avoid using local groups.** Make a strict policy to use domain groups for any system or application that integrates with AD. For

Identity Manager automates the workflow processes of entitlement requests and approvals.

systems and applications that cannot leverage AD groups, implement integration technologies to synchronize groups between AD and other systems, or Authentication Services, which allows Unix and Linux to leverage AD groups and users.

- **Identify overlapping groups, and re-factor and nest where appropriate.** An important part of every access-control remediation project is to identify duplicate groups and groups with a significant overlap in membership. Duplicate

groups need to be merged, and overlapping groups must be refactored (possibly with some limited nesting of groups introduced). To be deemed duplicate, two groups do not necessarily need to have exactly the same members. Perhaps the groups should have the same members but don't because of the aforementioned problems inherent to maintaining redundant information. Two groups may have a high degree of overlap in membership if they have different purposes. Examination of the members in common might reveal a third, previously unrecognized, role within the organization

- **Use a two-level group structure to separate roles and entitlements.** A group should either represent the type of users who make up its membership or the resource and access granted to the group; certainly the group can be named after only one of these. Therefore a widely accepted best practice is to create two types of groups. Create user groups to group users with a common role, team, department, responsibility, or project; name the group after that common demographic (for example, Board Members). Create resource groups to grant access to specific resources, and name the group after that resource and the permission granted (for instance, Financial Reports - Update). It is not unusual for the quantity of groups to approach the quantity of users in an organization.
- **Document group purpose, ownership, and details.** The criteria for membership in a user group should

be unambiguous. If the name alone cannot make this unambiguous, then additional information should be documented on the group itself, such as in the description or notes fields available in AD. Likewise, it should be easy to understand in definite terms exactly what a resource group provides access to. This information usually needs to be documented on the group, in the description or notes fields.

Three: Enforce business rules but handle exceptions flexibly and securely.

Your access control structure should reflect the business rules that drive it, yet remain flexible enough to securely handle the inevitable exceptions that arise. When you look at entitlements, the groups' names, notes, and membership should show not only who has access to what but also why they have that access. For instance, Deb, Chris, and Terry don't have submission access to the Marketing Communications system just because they are Deb, Chris, and Terry, but because they are all marketing product managers.

But there are exceptions, especially in small businesses and divisions. Perhaps John needs authority to submit to the Marketing Communications application because of just such an exception. Your access control structure needs to manage such a situation gracefully. You should not need to create an artificial group or role just to accommodate an unusual, "one-off" situation. However, such unusual exception entitlements should stand out as such. Figure 3 shows how such an exception might be implemented by simply making John a direct

member of the group Marketing Communications - Submit.

Unfortunately, AD does not allow you to add an explanatory note documenting the reason for or approval to a membership relationship, nor can you put an expiration date on the relationship. These are both examples of the problems that you can solve with Identity Manager's approval processes and Active Role's temporary group feature.

Four: Require entitlements to be approved by a designated data owner.

AD does not provide a way to document entitlement approvals.

Governance and nearly all regulations mandate that management establish a framework for controlling access to the organization's information resources. For accountability purposes, entitlements must be driven by business rules and approved by a responsible business person.

This best practice is particularly difficult to implement. As noted earlier, AD does not provide a way to document entitlement approvals. When looking at a group, you simply see that a certain set of users are members. There is no record of who approved those entitlements or when they occurred.

Manual workarounds are inefficient and often ineffective.

Some organizations adapt help-desk ticketing systems, retain

emails, or use collaboration software to fill this gap. But these approaches are essentially workarounds and result in crucial security information being maintained manually in a disconnected system.

Automating entitlement request and approval processes

Identity Manager automates the workflow processes of entitlement requests and approvals. The product's self-service approach speeds up the entitlement process while automatically creating all necessary documentation for governance purposes and ensuring that security processes and accountability are enforced. And Starling IARI provides a clear picture of precisely who has rights to what, and how those permissions compare to peers and even other similar organizations.

Automating the re-certification process for entitlements

Entitlements need to be periodically re-certified by attestation of responsible data owners. This process typically creates a manual-work burden for IT staff, in the form of manual report generation and distribution, as well as tracking of responses by data owners. Identity Manager automates this process; the solution already knows the information resources within the organization, their data owners, and current trustees.

IARI provides the ability perform "micro-certifications" on users' rights as managed through Active Roles in AD and AAD. This capability

ensures that the entitlements users have are actually those necessary for their job as approved by the line-of-business.

Five: Ensure that job changes and other relevant events trigger re-evaluation of entitlements.

A user's entitlements naturally expand during her tenure with the organization. Unless key lifecycle events trigger re-evaluation, inappropriate residual access and separation-of-duty issues will eventually form. These might go undetected until (hopefully) the recertification process discussed earlier catches the problems.

Therefore, organizations must build triggers into the business processes that process events such as the following:

- Job changes
- Termination
- Project completion

This is historically one of the most difficult areas in which to get cooperation from human resources and user departments. For that reason and for efficiency, automatically detecting these events is crucial. Active Roles can monitor record changes in human resources and other systems and use that information to automatically make changes to AD objects or otherwise trigger workflows. And IARI, detects and alerts on instances of entitlements rapidly increasing or being out of line with peers or policy.

One Identity solutions enable governance, reduce cost and manage risk

Overview of One Identity solutions that can help you follow best practices for access control

A number of One Identity products directly address the challenges that are inherent to access control in the AD-centric organization so common today:

Product	Description	Commandments
Identity Manager	For the entire enterprise, including AD	1-5
Active Roles	Secure, least-privilege administration and management of AD	2, 3
Authentication Services	Active Directory Bridge Technology for Unix, Linux, and Mac OS X	2
Identity Analytics & Risk Intelligence	Asses entitlement risk and remediate issues	4, 5

Identity Manager makes it easy for organizations to enable business users—instead of IT—to determine whether users' access requests should be granted.

About Identity Manager

In particular, Identity Manager makes it easy for organizations to follow the recommendations in this paper.

In most organizations, IT bears the burden of determining whether a user's access requests should be granted, even though IT lacks the information needed to avoid potential compliance

violations. Ideally these tasks should be delegated to the business users who understand the context of the requests—but this cannot be accomplished without relinquishing control of AD.

To securely move access request, approval, and attestation to end users and their managers, strong assurances and parameters

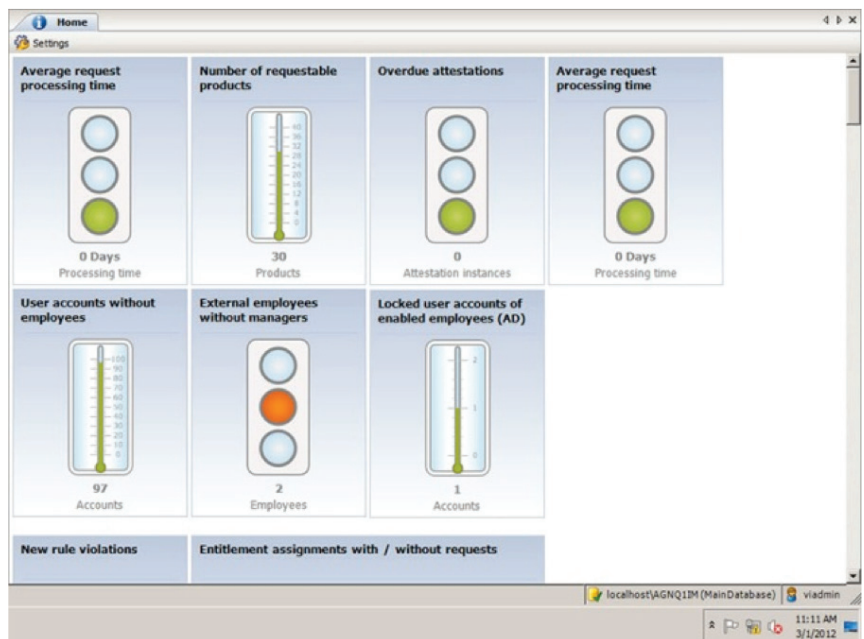


Figure 4. Identity Manager includes a summary dashboard that displays the status of AD group or distribution list attestation.

Good access governance involves cataloging your resources, identifying who can best make decisions about access to each resource, and automating as much as possible of the approval and periodic review processes.

need to be established to ensure that all actions and requests are fulfilled in a safe and secure manner. With AD self-service, the burden of user access requests can now be transferred from your IT staff to business owners without sacrificing security, compliance, and governance objectives.

Identity Manager includes the following features:

- **Access request portal**—End users can request AD group and distribution list access via a customizable online portal, which automatically flows to the appropriate group owner in accordance with established policy. Approved requests can be automatically fulfilled, removing the burden from AD administrators.
- **AD group attestation engine**—Business managers or group owners can schedule routine or on-demand attestation of AD groups and distribution lists, to ensure and maintain compliance.
- **Summary dashboard**—A clear and concise dashboard displays the status of AD group or distribution list attestation. You can produce detailed reports for discovery and to prove compliance.
- **Assigned ownership**—Ownership of specific groups or distribution lists can be assigned to key individuals in the organization, based on their business needs and organizational roles, thus reducing the risk of orphaned groups.
- **Customizable portal**—You can easily customize the end-user access-request portal to ensure usability and adherence to corporate branding requirements.
- **Self-service**—Empower your end users and managers to complete the most labor-intensive AD group-

related tasks on their own, without administrator involvement, while leveraging predefined approval processes and workflows. Full customization enables you to manage workflows and retain control over the parameters.

- **Fast time to value**—Avoid the challenges of adopting a customized AD group-management solution. One Identity solution's flexible architecture ensures that deployment will be a simple configuration exercise.

Conclusion

Good access control depends on avoiding the use of local groups and instead assigning permissions to AD groups. Good access governance involves cataloging your resources, identifying who can best make decisions about access to each resource, and automating as much as possible of the approval and periodic review processes. AD has emerged as a core repository to hold this information. But organizations will experience increased cost and governance difficulties if the accesscontrol processes that maintain identity and access control objects in AD are not automated. Identity Manager provides this automation.

Eliminating redundant groups figures heavily into good governance and effective access control. However, some applications and systems still do not integrate with AD. Furthermore, key events in the user-account lifecycle occur outside AD—and historically lead to inappropriate residual access or violation of separation-of-duty controls. Integration

products such as Authentication Services solve these problems by synchronizing changes and automatically triggering workflows when access-control events occur.

As the core of identity and access control within most organizations, AD itself needs protection and accountability. Active Roles acts as a virtual firewall around AD, enabling you to control access

through delegation, using a least-privilege model. Based on defined administrative policies and associated permissions, Active Roles generates and strictly enforces access rules, eliminating the errors and inconsistencies that are common with native approaches to AD management. Plus, robust and personalized approval procedures establish an IT process and oversight that

are consistent with business requirements, with responsibility chains that complement the automated management of directory data.

One Identity solutions help an organization follow best practices while simultaneously increasing responsiveness and reducing the burden on IT.



For More Information

© 2017 One Identity LLC,
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC.

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS

PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats.

For more information, visit oneidentity.com.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC

Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.oneidentity.com) for regional and international office information.