# Active Directory Security Groups vs Distribution Groups

blog.netwrix.com/2023/04/28/active-directory-security-groups-vs-distribution-groups

Kevin Joyce

Using groups is a best practice for Active Directory management. This article describes the two types of Active Directory groups — security groups and distribution groups — and offers guidance for using them effectively.

## Key Differences between Security Groups and Distribution Lists

Security groups and distribution groups (more commonly called distribution lists) are both Active Directory groups, but they are designed for very different purposes:

- **Security groups** are used to manage user and computer access to shared IT resources, such as data and applications. Permissions are assigned to the security group, and all user and computer accounts that are members of the group have those permissions automatically.
- **Distribution groups (distribution lists)** are used for sending emails to a set of users, without the sender having to enter each recipient's email address individually.

Note that while you can use security groups for email distribution, you cannot use distribution lists to assign permissions.

Now, let's dive deeper into each type of AD group.

## Security Groups

Active Directory security groups are used to manage user and computer access to shared resources, such as folders, applications and printers. This makes provisioning easier and more accurate. For example, when a new person joins the organization, the IT team can quickly grant them access to exactly the resources they need to do their job simply by adding them to the appropriate security groups, such as the groups for their department and their specific projects. Security groups can also be set up to deny a set of users access to a particular resource.

Two primary functions of a security group are:

- **Assign User Rights:** Assigning user rights to a security group determines what the members of that particular group can do within the scope of a domain. For example, a user who is added to the Backup Operators group can back-up and restore files and directories located on each domain controller in the domain. By being a member of this group, you inherit the user rights assigned to the group.

- **Assign Permissions for Resources:** This is different from user rights because user rights apply across an entire domain versus permissions that are directed to a specific entity. Permissions determine who can access the resource and the level of access, such as Full Control or Read-only.

Simply put, user rights apply to user accounts while permissions are associated with objects.

Administrators can create security groups and manage their permissions and membership through multiple methods, including the Active Directory Users and Computers (ADUC) console, Windows PowerShell, and third-party group management software solutions.

## What are Active Directory Security Group Permissions?

Permissions in Active Directory are a set of rules and regulations that define how much authority an object has, to view or modify other objects and files in the directory. To ensure that users only have access to the resources they need, IT administrators assign permissions through Access Control Lists (ACLs).

## What are Access Control Lists (ACLs)?

Access Control Lists define entities that have access to an object and the type of access. These entities can be user accounts, computer accounts, or groups. For example, if a file object has an ACL that contains (Mary: read; Sarah: read, write), it would permit Mary to read the file and permit Sarah to read and write it.

An Access Control List can be configured on an individual object or an organizational unit (OU), which means all the descendent objects of the OU inherit the ACL.

### Types of Access Control Lists

There are two types of ACLs, each of which performs a distinctive function:

- **Discretionary access control list (DACL):** This list states the access rights assigned to an entity over an object. When an entity or a process attempts to access an object, the system will determine access based on the following:
    - If an object does not have a DACL, the system allows everyone full access to it.
    - If an object has a DACL, the system allows the access that is explicitly allowed by the access control entries (ACEs) in the DACL.
    - If a DACL has ACEs that allow access to a limited set of users or groups, the system implicitly denies access to everyone not included in the ACEs.
    - If an object's DACL has no ACEs, the system does not allow access to anyone.

- **System access control list (SACL):** This list generates audit reports that state which entity was trying to gain access to an object. It also states if the entity was denied access or granted access for that object along with the type of access provided.

### Tip: Avoid using Security Groups for Sending Emails

In a normal setup, distribution groups created in Exchange and Microsoft 365 are assigned email addresses by default but security groups are not. Accordingly, security groups cannot normally be used for email distribution. However, it is possible to mail-enable a security group in order to use it for both granting access to resources and sending emails.

Nevertheless, it is not a good practice to use security groups for email because doing so could compromise security. A mail-enabled security group enhances the risk of identity theft for itself first, which could spread to other security groups that are members of the compromised group. Or for instance, if a mail-enabled security group receives a malicious link in a message, it might intrude your organization's privacy by disrupting certain settings.

If you have a requirement to send an email to all members of a security group, it is best to create a distribution group with the same membership as the security group.

## Distribution Groups

Active Directory distribution groups are used to send emails to a group of users rather than to individual recipients one by one. For instance, a company might set up a distribution list for all employees, another distribution list for all managers and a separate distribution list for each department. When you want to send an email to any of these groups, you can simply select the distribution group, instead of having to add all the recipients individually. This saves time and improves accuracy.

As noted earlier, you cannot assign permissions to distribution lists.

### Distribution Groups vs Shared Mailboxes

A distribution list is quite different from a shared mailbox. A shared mailbox is used when multiple people require access to the same mailbox. For instance, the helpdesk team and the IT support team might use a shared mailbox so that they can collaborate on tasks. Moreover, anyone on the teams can send and receive emails on behalf of the teams. Typically, a shared mailbox has a generic address like "ITsupport@company.com" so that it stays the same even as the makeup of the team responsible for it changes over time. When a user sends an email from a shared mailbox, it is sent from the shared mailbox address rather than the user's own email address. A copy of that email is sent to the shared mailbox for all the other members to see.

One scenario that highlights the difference between a distribution list and a shared mailbox is email deletion. If a user deletes an email from a shared mailbox, that email is deleted for everyone who has access to that mailbox. But when a member of a distribution list deletes an email sent to the group, that email is not deleted from the mailbox of any other recipient.

## Can Distribution Groups be Managed by Security Groups and Vice Versa?

A security group can be made the owner of a distribution group. Doing so would empower all members of the security group to manage that distribution group — for example, its non-delivery report recipients and send/receive message restrictions. For example, a security group created for a project team might be the owner of its associated distribution list, and the corporate communications team might be the owner of multiple distribution lists for the company.

On the other hand, a distribution group cannot be made the owner of a security group.

## Is it Safe to Delete Distribution Groups and Security Groups?

Deleting a distribution group does not pose a threat to your organization's security, though accidentally deleting one can disrupt communications until the group can be restored from backup or a new one is created and populated with the same members.

Deleting a security group, however, can have serious implications, such as:

- **Security** — Deleting a security group that restricts members' access to certain resources would grant those users access to those resources.
- **Productivity** — Deleting a security group that grants its members access to certain resources would leave users unable to access the data and applications they need to do their jobs.

Accordingly, be cautious about deleting security groups.

## Conclusion

Keeping your security groups and distribution lists accurate and up to date is critical to security and business continuity. To simplify the work, consider investing in a solution like Netwrix GroupID. Netwrix GroupID makes it easy to ensure that:

- Every group in your directory serves a purpose.
- Every group has an owner.
- Users are not granted unnecessary membership in groups.
- No groups have excessive permissions.
- Groups do not outlive their intended purpose.
- Duplicate groups do not exist.

Kevin Joyce
Senior Technical Product Manager at Netwrix. Kevin is passionate about cyber-security and holds a Bachelor of Science degree in Digital Forensics from Bloomsburg University of Pennsylvania.