# Securitay Inc.

# *Whitepaper*: Self-Service Group Management

***October 31, 2006***

## *Audience*

This paper is a guide for IT specialists, Business and Technical decision makers looking to improve the efficiency of their organizations through self-service group management. In this paper we will discuss the uses of Active Directory Security Groups and Distribution Lists along with an explanation of why all knowledge workers in your organization should have the ability to manage them.

## *Self-service for Active Directory Security Groups*

Several of the basic roles of Windows Server involve publishing resources to a network so that personnel in your organization can use them. These resources might be file shares, printers, or web applications hosted on Windows Internet Information Services. For all but the smallest companies, there are usually security policies that dictate restrictions about who has access to sensitive information. To restrict access, Microsoft Windows Server-hosted resources such as those above support Access Control Lists (ACLs). ACLs specify the access level to which a user has access to a resource. Other applications use ACLs as well, including Microsoft SQL.

The only native interface provided by Windows to manage security on such resources is the Security tab on the object Properties Microsoft Management Console (MMC) snap-in. The problem with this is that managing access privileges by giving individual users access to resources through the snap-in is a time-consuming and error-prone process. For those familiar with managing access through the Properties MMC snap-in, we don't have to belabor the point that this interface is not always user-friendly or intuitive. As you can see from just the screenshot below, the interface has quite a few options.

 

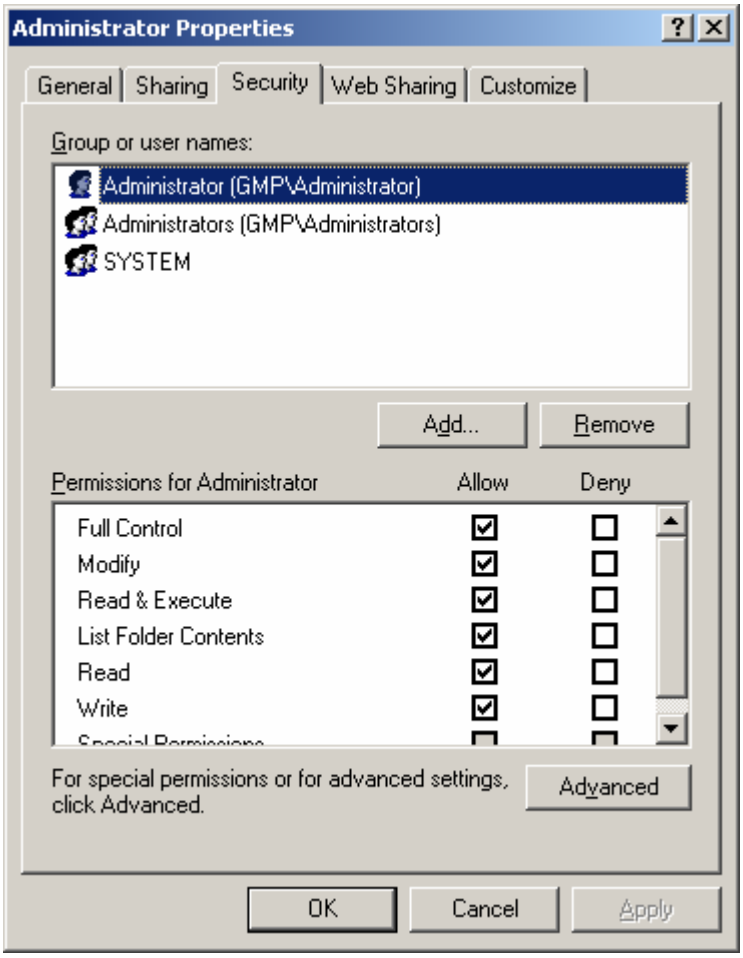


*Figure 1: Security tab on File Properties MMC snap-in*

The management burden of having a poor interface is multiplied, however, because in most organizations access privileges change frequently as employees change roles and responsibilities in the organization. If you were to manage access to resources by managing the ACL on every specific resource then huge amounts of administrative time would be consumed simply through adding and subtracting user rights through the security tab.

Microsoft Active Directory Security Groups provide a very powerful tool with which to manage access to typical network resources such as those mentioned above. They work by collecting users with similar access privileges into a single management entity and by using that entity, the security group, to grant the appropriate level of access to the resource. By using security groups, management overhead for even relatively small numbers of resources and users can be greatly reduced.

For example, consider a small branch office with 10 employees and local resources including a file server, a printer, a LOB application, a Sharepoint portal and a local database for a total of five resources. All of the employees in this scenario have read/write access to these resources, but employees change branch locations frequently

and the security policy for this organization requires that only employees currently assigned to the branch office should have access.

If access is managed on each resource directly, then a single employee leaving the branch would require that all five applications and resources be reconfigured through its unique management interface (with its own unique definition of read/write access means!) to remove the employee's access. The chance that one of these operations will be done incorrectly or forgotten is high for a single instance and almost guaranteed over time. If security groups are used to control access, however, a single change to the membership of the group will remove access from all of the resources and the resource administrator only has to worry about establishing the correct set of rights to grant once.

Even this example of a very small organization shows why Active Directory security groups are necessary for effective management of access to network resources. Given the ability for security groups to improve information manageability, what is needed next is an improvement in how the security group itself is managed. Although in the example above it only takes one operation instead of five to take a user out a group, the Active Directory MMC snap-in for managing Users and Computers (ADUC) is not an ideal interface.

One of the reasons it is not an ideal interface is that it is designed to be used primarily by highly trained system administrators. The ADUC MMC is fairly complicated and also allows the possibilities of serious error if the administrator gets careless. There are plenty of stories about AD administrators who "accidently" dragged an Organizational Unit with thousands of users from one domain and dropped it in another. For this reason, most organizations have very strict policies around administering accounts in ADUC and this includes managing group membership. But there is really no reason why the IT administrators should have to be involved in a simple operation such as group membership management.

An ideal situation results if the management of groups can be delegated to business owners instead of IT. If the business owner can be provided with tools that allow the simplified management of resources that they own, then they can be more responsive to the needs of their own users. By being more responsive in removing access as well as granting access, the organization will also become more able to comply with regulatory requirements and internal security policies. **Securitay's *Group Management Portal*** provides just such a mechanism.

## *Self-service for Distribution Lists*

Microsoft Exchange is a powerful tool for collaboration and communication amongst large numbers of users, but suffers inefficiencies if each mail that someone sends must contain the e-mail address of everyone that should get the mail. Examples are easy to come by. Consider what would happen if the CEO of General Electric wants to send a mail to every single person the company but there were no distribution lists! The typical

 

solution for organizations that use Microsoft Exchange is to create e-mail distribution lists that reflect the organizational relationships of users. Similarly, e-mail is a valuable tool for more temporary collections of users. For example, consider a project team pulled together from employees across a company's different divisions. Again, the typical solution is to create an e-mail distribution lists with each employee assigned to the project added to the list.

Most users are aware of the utility of distribution lists, but are often frustrated at the inability to get them created in a timely manner. Some organizations have multiple week backlogs of such requests waiting to be granted. For teams that only exist for a period of months, waiting weeks for IT to create a distribution list that will improve team communication is not adequate. It is important for an organization's IT infrastructure to be able to support opportunistic approaches to doing business and if this can be accomplished while reducing costs then the solution is doubly attractive.

It is therefore essential that organizations provide their employees the ability to rapidly and efficiently form ad-hoc working groups. While ad hoc collaboration is an important part of a flexible and opportunistic organizational strategy, today's regulatory environment and the potential risk to the business when critical data is lost or exposed to evil-doers, means that tools must be made available to the average user that allow them to collaborate securely.

The proper tool providing this functionality allows end-users to navigate to a web site and manage their own group and distribution lists (DLs) memberships, create new groups and DLs, and monitor workflow activities associated with these actions. The tool should be simple to use, providing the user with the ability to quickly do the tasks required without introducing technical jargon. The tool should also be simple to deploy and manage because one of the goals is to offload administrative overhead, not switch the overhead from one task to another.

Securitay's **Group Management Portal** fulfills all of these requirements and many more as well, all at an exceedingly attractive price point. Built using the latest development tools that greatly reduce development time while enhancing reliability, the Group Management Portal is simply the most cost effective solution on the market while matching or exceeding the feature set of similar products.

Built to interact seamlessly with Microsoft's *Active Directory* and *Exchange*, the **Group Management Portal** is easy to deploy and configure, usually providing full operational capability in as little as eight hours from the start of an installation to the end of configuration. Your requirements are simple – shouldn't you have a tool that is simple to use, deploy and maintain?

## *Group Management Portal Application Walkthrough*

We think that our application speaks for itself in the way it is designed and the way it is designed to be used. As you review the capabilities of this straight-forward but powerful tool we think that you'll agree that it's the right tool for your organization.

The following section will describe the capabilities and interfaces of the **Group Management Portal** by describing the tasks that can be performed with the application**.**

### Task: Manage Group Memberships

The application home page (default page) for the user is the summary screen that displays all the security groups and distribution lists (DL) that the user is currently a member of along with the status of any pending requests to join a secured group or DL.

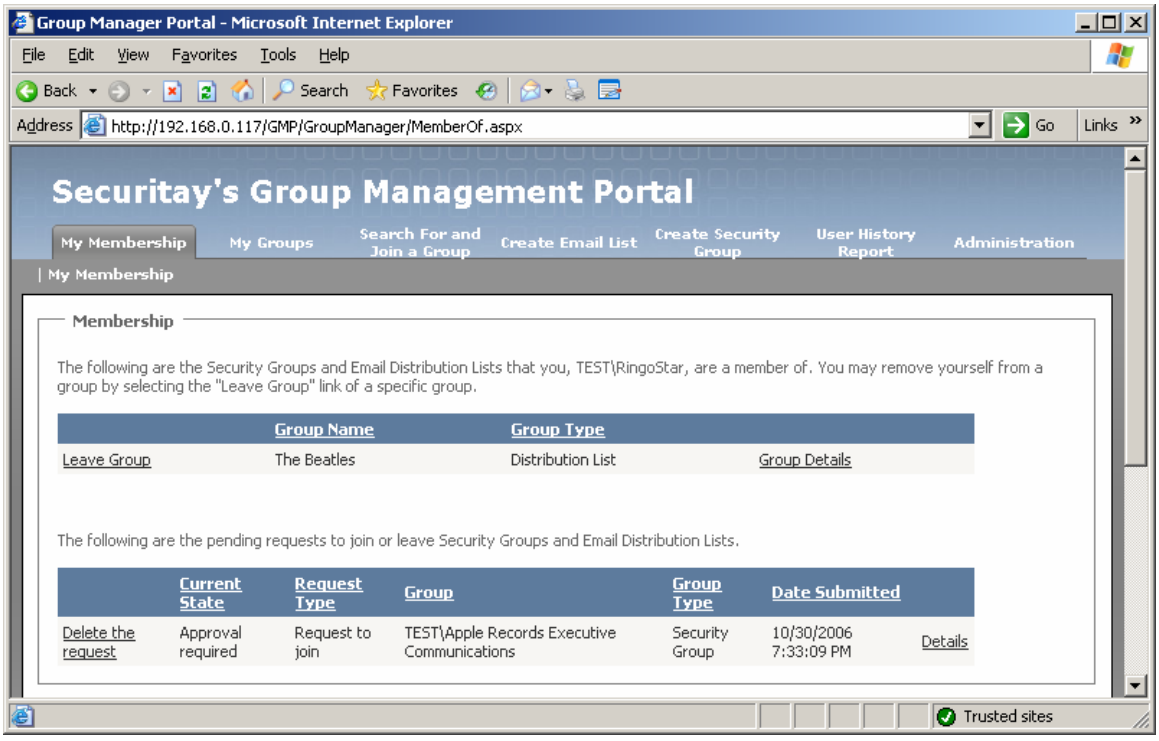


*Figure 2: Group membership summary*

With a single click, users can remove themselves from any group or distribution list that they currently are a member of. With another click, users can examine the details of any group they are a member of. The group/distribution list details screen is explained below.

Securitay's **Group Management Portal** product does not store any information about Group or DL memberships itself and instead uses Active Directory as the authoritative store. This means that there is never a data synchronization problem between what the application thinks the state is and what's actually in Active Directory. This also means that administrative actions on Groups and Users through the Active Directory MMC are

always authoritative and will be reflected immediately in the Group Management Portal web interface.

## Task: Review and Edit Group Settings

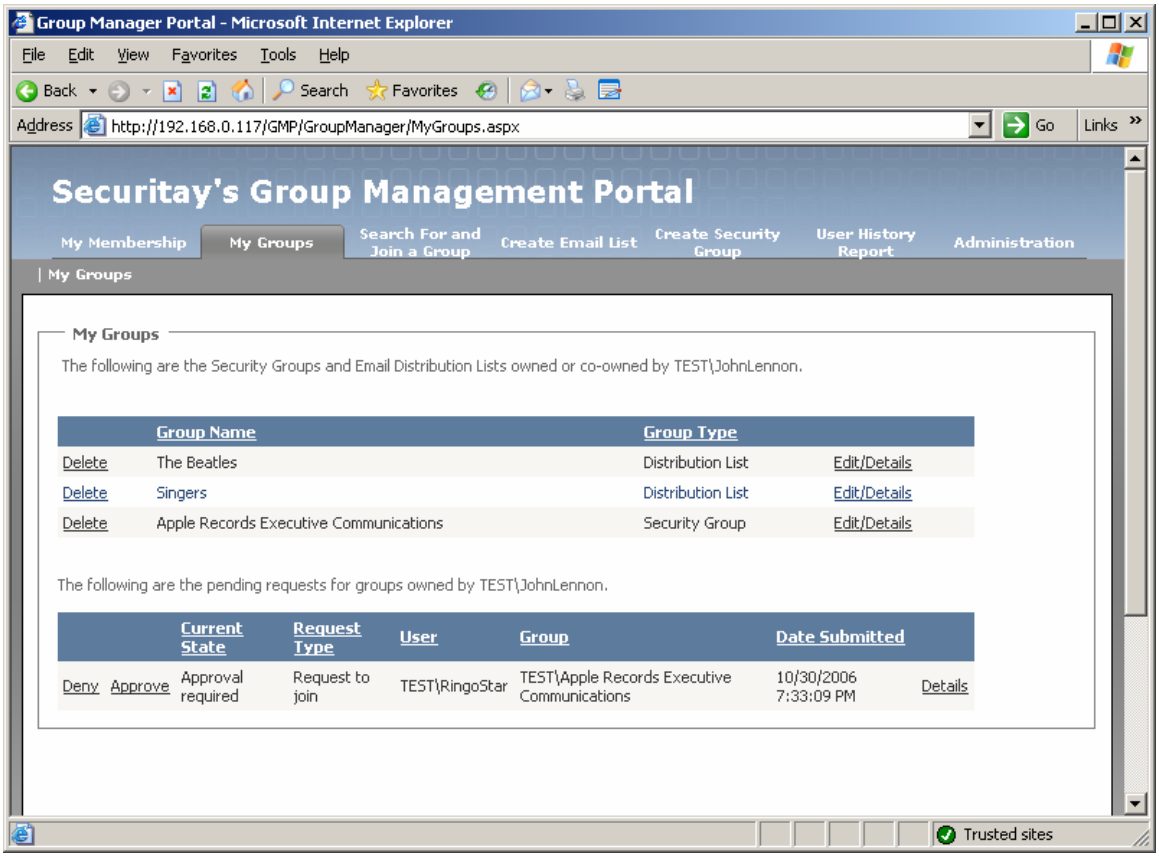


*Figure 3: Manage groups and distribution lists*

This screen allows an end user to review, edit, and administratively manage membership in any group that they own or co-own. By clicking on the **Edit/Details** link, the user can change the settings of a security group or DL including the name of the group, membership, workflow requirements, etc.

The **Edit/Details** screen is basically identical to the **Create Security Group** and **Create Distribution List** screens and more details on these screens are provided below.

## Task: Approve Membership Change

If a group or distribution list is configured with the **Approval Required** workflow option, the owners and co-owners of a group are automatically notified through e-mail that there is a request for a change to that group's membership. By clicking on the link in

the e-mail or by navigating directly to the screen shown above the owner or co-owner can review all pending requests and approve or deny the request as desired.

The user can review the details of any pending request including the business justification supplied by the requestor. As shown above, Ringo has submitted a request to join a security group owned by John. John can choose to review the details of the request before taking action.

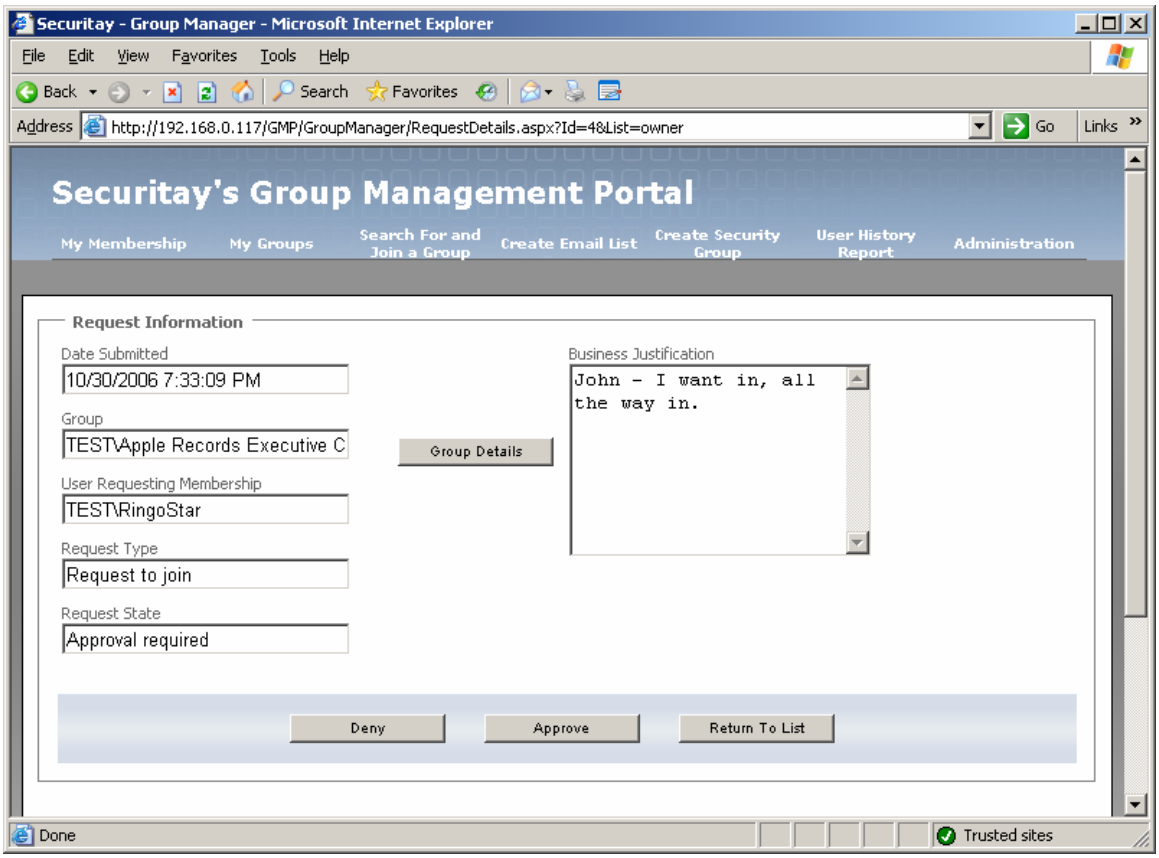


*Figure 4: Membership request details*

Once the details of the request have been reviewed, the user can choose to Deny or Approve the request which will generate a notification to the user who made the request.

## Task: Join a Group or Distribution List

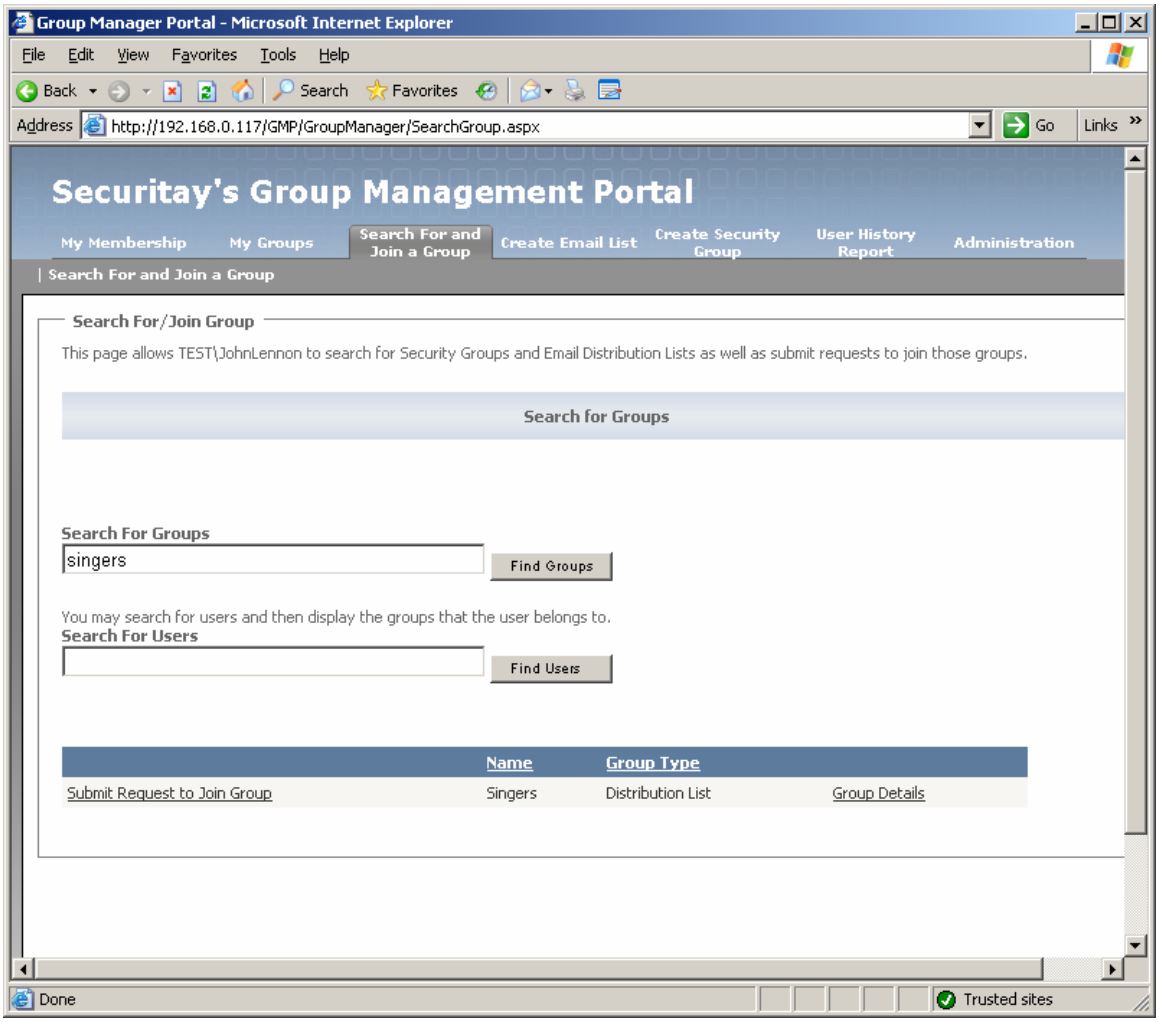


*Figure 5: Join a group*

Once the capability to collaborate through e-mail and task portals becomes commonplace in a organization, the ability for a user to add themselves to the appropriate security group allowing access to project materials or to a distribution list where communication takes place is critical. Allowing users to manage their own memberships without having to involve IT is a time saver for both the user and for the always over-burdened IT staff. Group Management Portal allows a user to join a group through two convenient mechanisms.

## Sub Task: Join a single group

If any part of the name, display name, key words, or description of the group is known, then the Group Management Portal applications lets a user join that group or DL with but a single click. Note that all workflow rules associated with that group are obeyed, so that the request to join a group might be granted immediately or will be granted when the proper approvals are performed.

## Sub Task: Join multiple groups that another user is a member of

Group Management Portal has a powerful feature that allows a user to join any number of groups that another user is already a member of. This capability aligns with typical on-boarding processes where a new employee can be instructed to join all of the groups that his or her mentor is a member of – subject to workflow rules, of course! For this example Ringo has found out about the Group Management Portal and decides that he should be a part of every group that John belongs to.

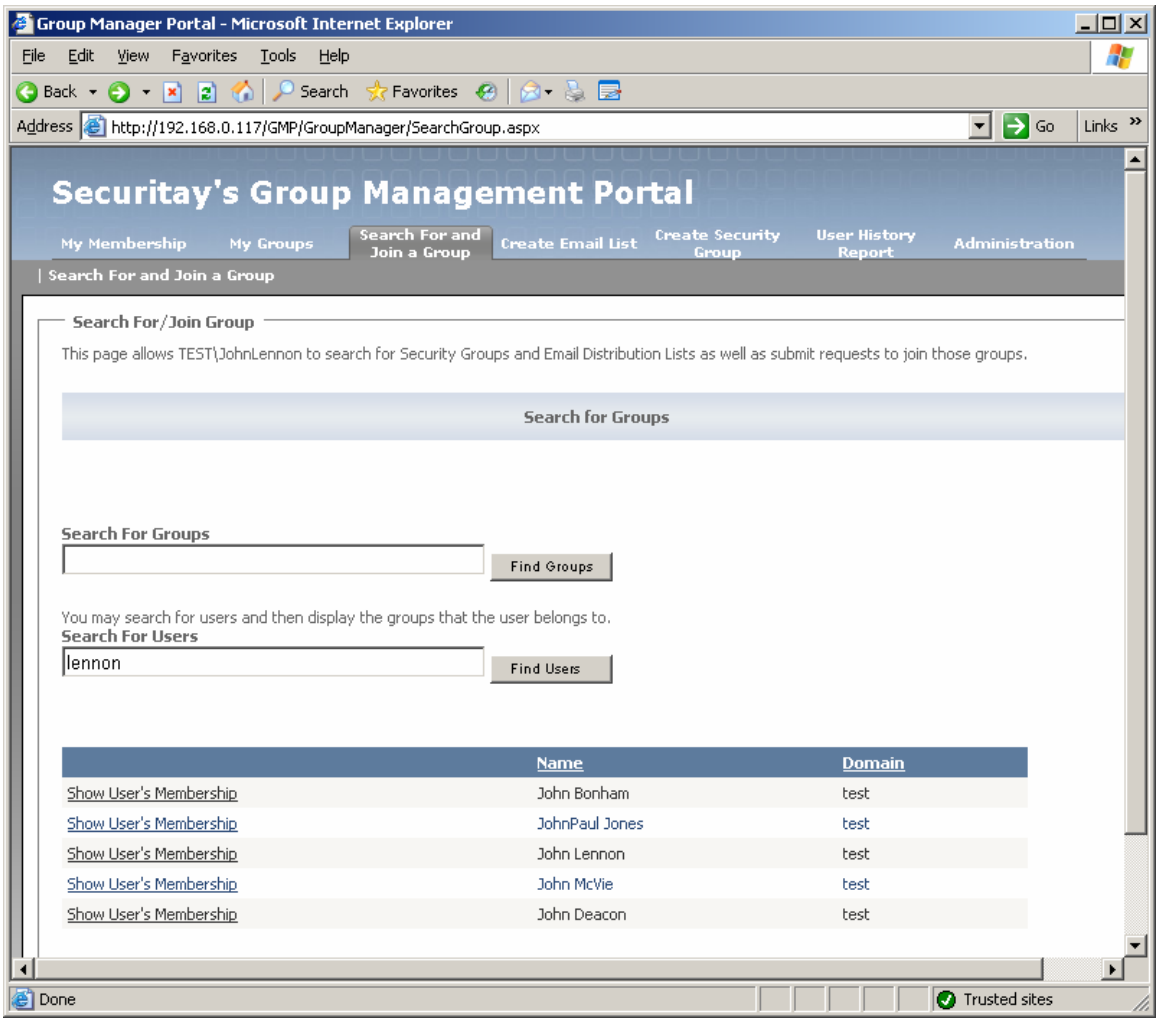


*Figure 6: Select a user to see the groups they belong to*

From this screen Ringo can click on **Show User's Membership** next to John Lennon's name and the following screen is displayed.

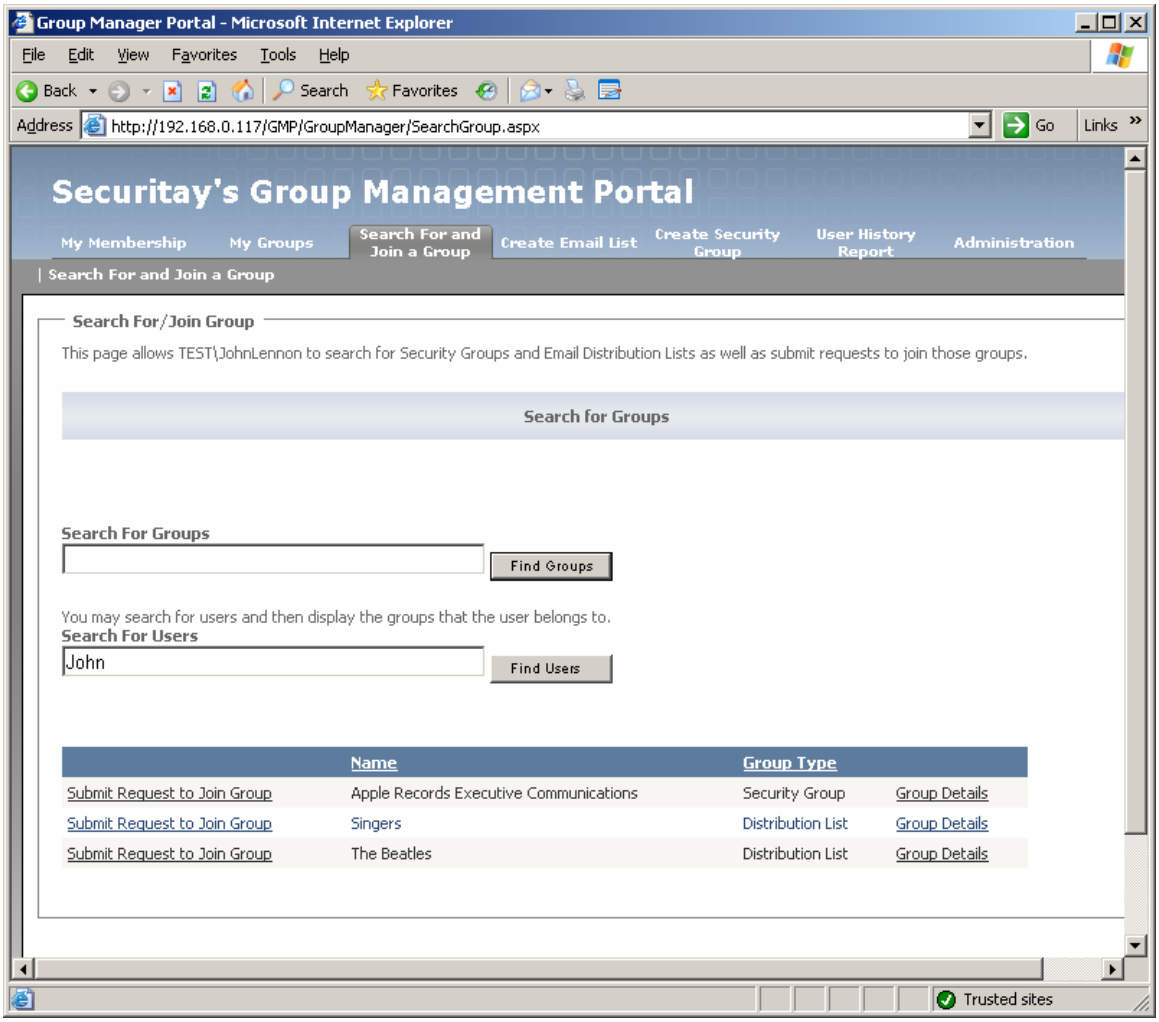


*Figure 7: Request to join groups that another user belongs to*

Ringo can now click on **Submit Request to Join Group** for each group or distribution list he wants to become a member of. Depending on the workflow configuration for the group or DL Ringo might see the following:

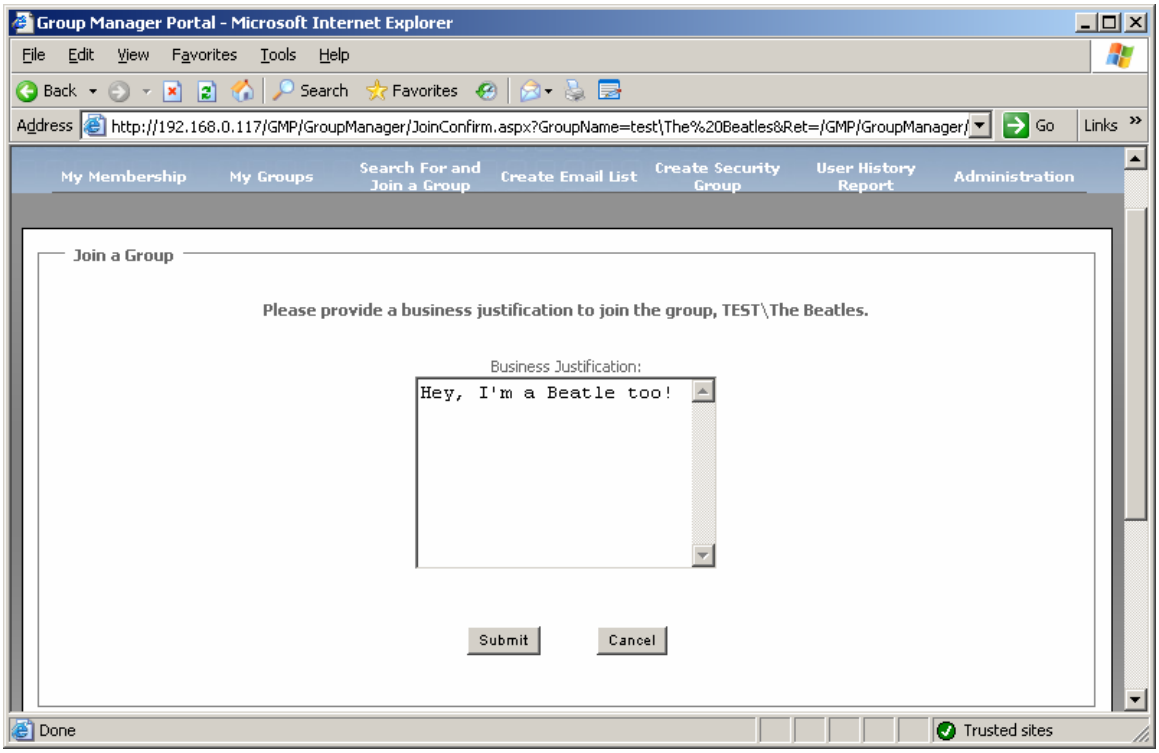


*Figure 8: Provide business justification*

When Ringo provides the appropriate business justification, the request is submitted and Ringo will be returned to the previous screen where he can initiate additional requests to join other groups or DLs.

## Task: Create a Security Group

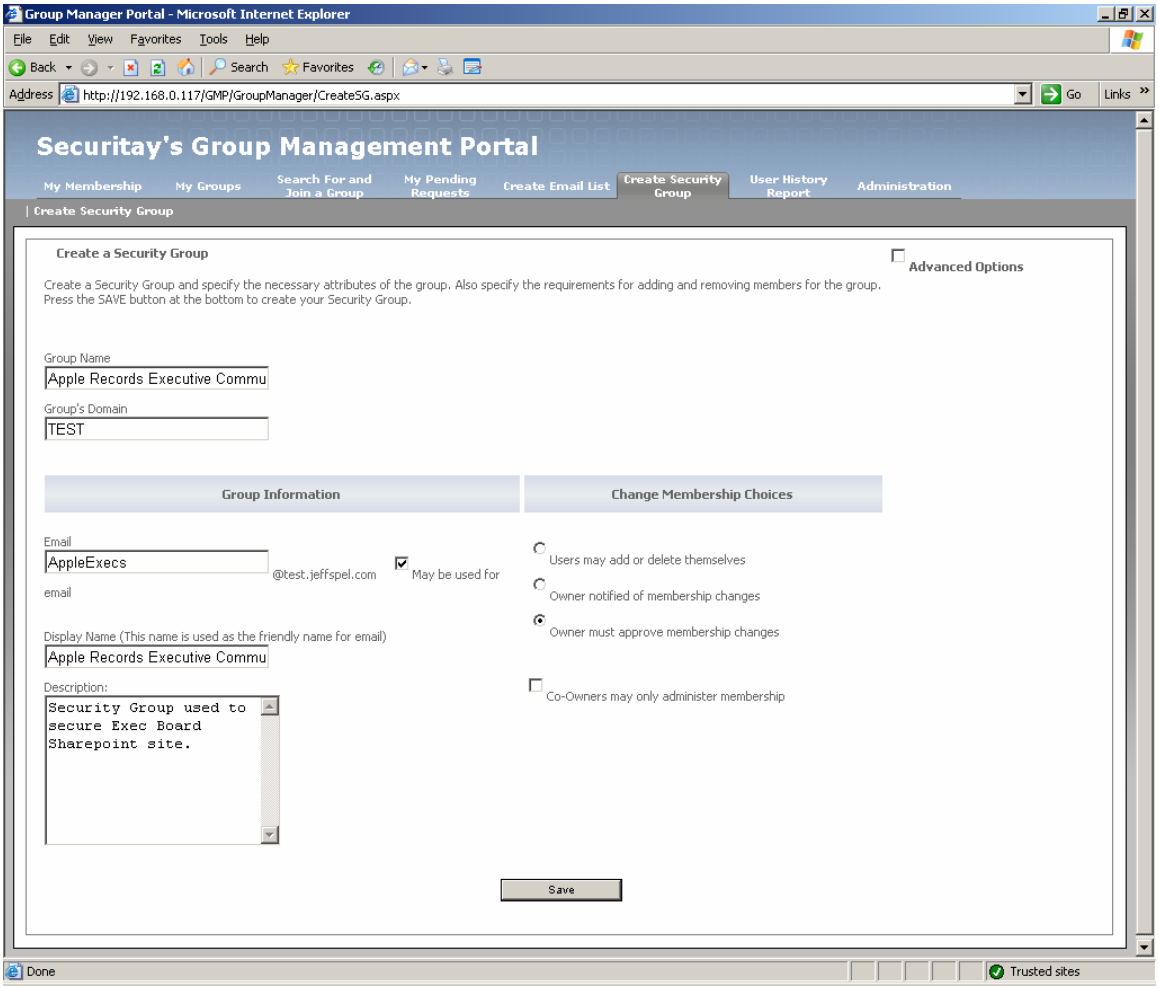

*Figure 9: Create a security group*

The Group Management Portal makes it very simple for any user in the organization to create security groups that are often needed for ad-hoc, business unit-level collaboration. Security groups are needed for easily securing access to important resources such as sensitive documents on a file share or a collaboration workspace in a Microsoft Sharepoint web site. While very simple, the interface provides the ability to easily associate typical workflows needed for group management actions with a specific group and collect additional audit-related information such as Business Justification.

## Task: Create a Distribution List

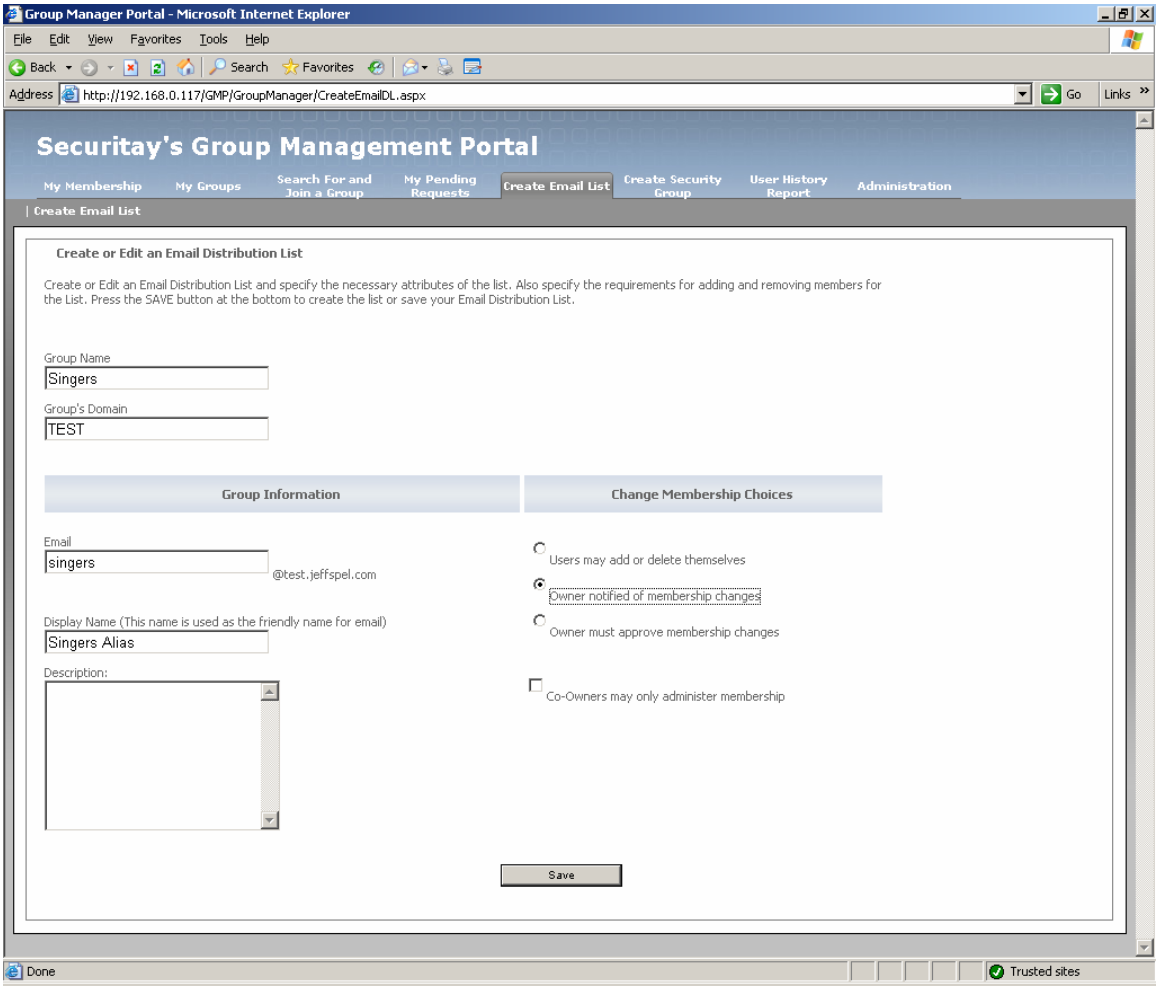


*Figure 10: Create a distribution list*

From an application perspective, creating a Distribution List is almost exactly like creating a Security Group. All the options are identical and have the same affect. The only reason that there are two screens for such closely related actions is to make sure the user does not get confused about what they are doing. Because of certain limitations in Windows with regards to users being a member of a large number of security groups, users should use distribution lists when appropriate.

## Task: Add Members to a Group or Distribution List

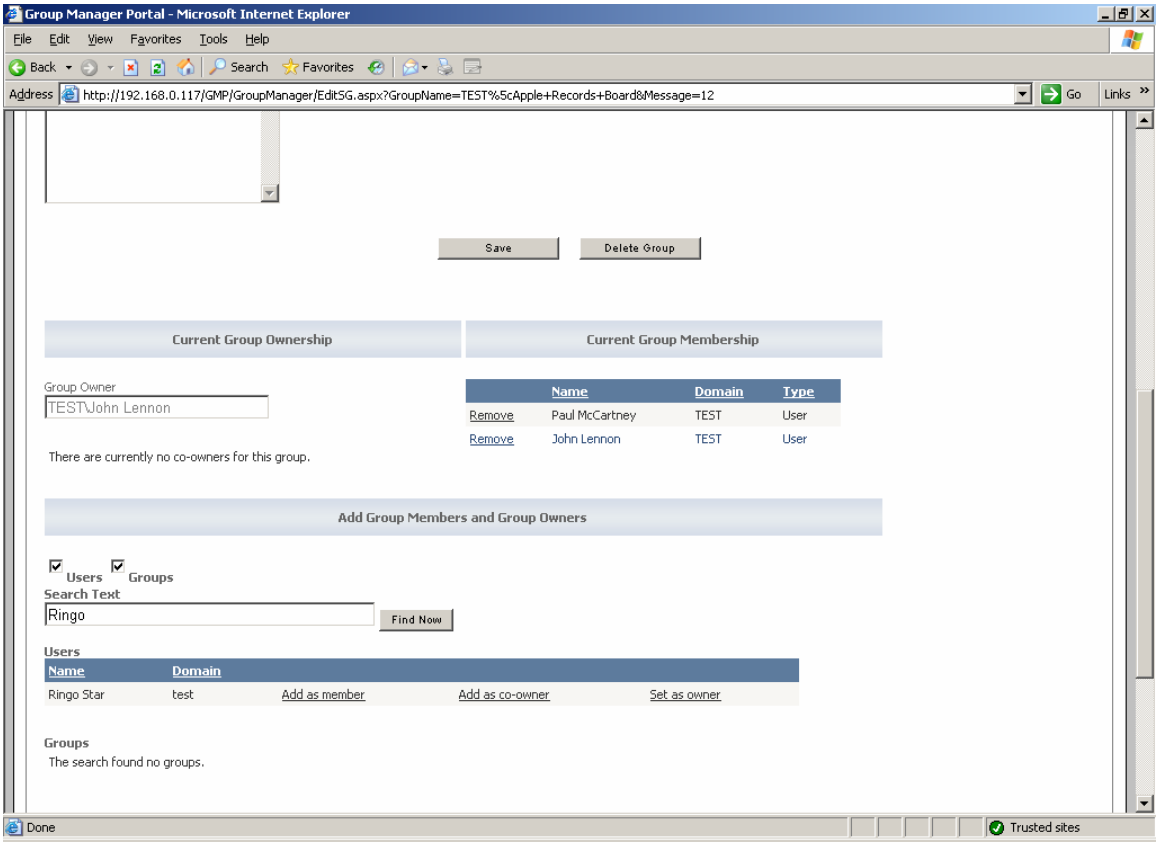


*Figure 11: Add members*

Once a group or distribution list is created it is a simple matter for the group owner to add members. From the **My Groups** screen click on **Edit/Details**. Scroll down until you see the "Add Group Members and Group Owners". In the text box you can type any portion of a users (or group's) account name and then click **Find Now**. The application will search Active Directory and show all possible users that match the text typed in the table below. In this case we will click on **Add as member** next to Ringo's name and add him to the Beatles distribution list.

## *Summary*

We hope you agree that Securitay's Group Management Portal is simply the best and easiest to use application of its kind on the market. We think that you'll find our pricing to be extremely easy on the budget as well. Please visit our website at www.securitay.com to find out more about our company, other products, and to download a no-strings attached demo version of the product. If you have any questions about the product, please don't hesitate to e-mail us at sales@securitay.com or call us at 425-392-0203.