Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

## Role based administration in ISA Server 2006

### Abstract

In this article, I will show you how to implement a role based administration model with Microsoft ISA Server 2006 for distributed administration.

### Let's begin

ISA Server 2006 allows the delegation of administrative permissions to individual users to make the Administration model more flexible. ISA Server 2006 uses two different models to assign permissions to individual users. ISA Server 2006 Standard uses a simple model that controls access for specific parts of the ISA configuration. ISA Server 2006 Enterprise uses a more distributed model which let you assign permissions at the Enterprise level and at array level.

| ISA Server 2006 Standard role | Tasks |
|---|---|
| ISA Server Monitoring Auditor | Users which has bee assigned to this role can monitor ISA Server 2006 but cannot view the ISA Server configuration |
| ISA Server Auditor | Users and groups assigned this role can perform all monitoring activities like Firewall log configuration, definition of ISA alerts and can view but not modify the ISA Server 2006 configuration |
| ISA Server Full Administrator | Users and groups can perform any ISA Server 2006 task. This is the most powerful role in ISA Server 2006 |

Table 1: ISA Server 2006 Standard roles

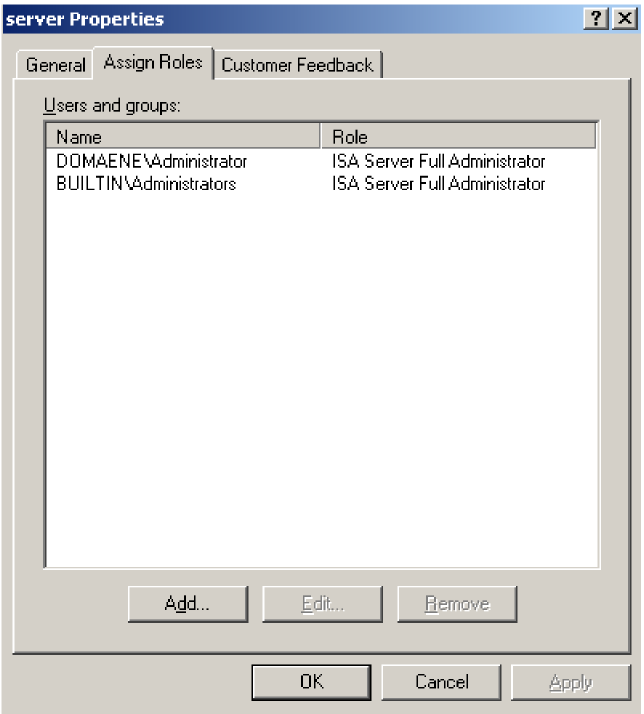
Every normal Windows user or Windows group can be assigned permissions for ISA Server roles. No special privileges or Windows permissions are required.

### Please note:

There is one exception to this I wrote above. When a user tries to open Perfmon for viewing the ISA Server 2006 Performance counters or the ISA Server Dashboard, the account must be a Member of the Windows Server 2003 Performance Monitor User group.

To assign administrative roles, start the ISA Server 2006 Management console; right click the Server objects properties and navigate to the Assign Roles tab. You must be an Administrator with the assigned role “ISA Server Full Administrator” to delegate permissions.

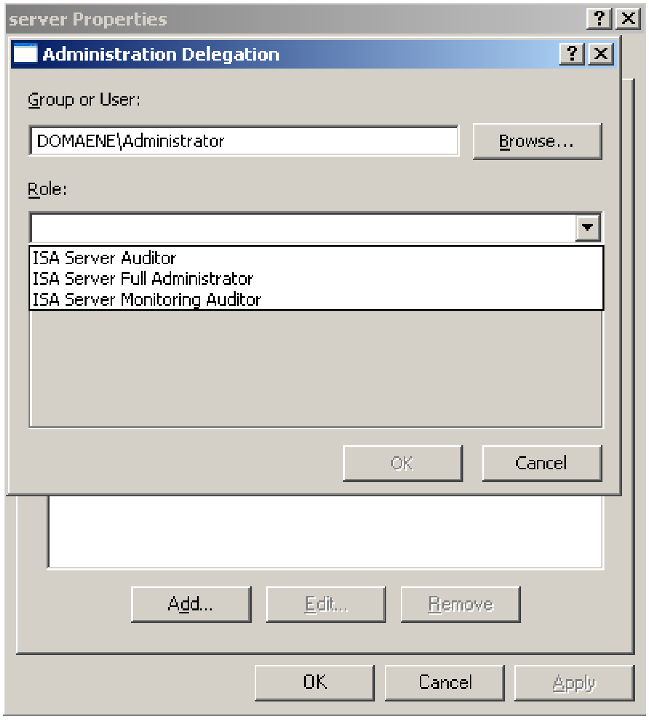
Click Add to select users or groups which you like to assign specific roles.



| Name | Role |
|---|---|
| DOMAENE\Administrator | ISA Server Full Administrator |
| BUILTIN\Administrators | ISA Server Full Administrator |

Figure 1: Assign ISA management roles

After selecting the user group or user, select the role that you want to assign to the user or user group.



Group or User: DOMAENE\Administrator

Role:

- ISA Server Auditor
- ISA Server Full Administrator
- ISA Server Monitoring Auditor

Figure 2: Select management role

### Example permission of ISA Server roles

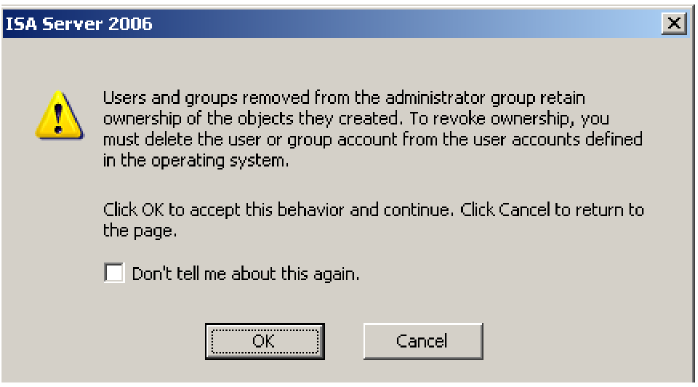
| Activity | ISA Server Monitoring Auditor | ISA Server Auditor | ISA Server Full Administrator |
|---|---|---|---|

| | | | |
|---|---|---|---|
| View Dashboard, alerts, connectivity, sessions, services | Allowed | Allowed | Allowed |
| Acknowledge alerts | Allowed | Allowed | Allowed |
| View log information | Not allowed | Allowed | Allowed |
| Create alert definitions | Not allowed | Not allowed | Allowed |
| Create reports | Not allowed | Allowed | Allowed |
| Stop and start sessions and services | Not allowed | Allowed | Allowed |
| View firewall policy | Not allowed | Allowed | Allowed |
| Configure firewall policy | Not allowed | Not allowed | Allowed |
| Configure cache | Not allowed | Not allowed | Allowed |
| Configure a virtual private network (VPN) | Not allowed | Not allowed | Allowed |

Table 2: ISA Server 2006 detailed permissions (Source: http://technet.microsoft.com/en-us/library/bb794769.aspx)

### Attention

If you remove the assigned ISA management role for a specific user or user group, the users removed from this group retain ownership of the objects they created, so that it is possible that an ISA Administrator can delete objects he created although the user is no more a member of an ISA Server role.



ISA Server 2006

Users and groups removed from the administrator group retain ownership of the objects they created. To revoke ownership, you must delete the user or group account from the user accounts defined in the operating system.

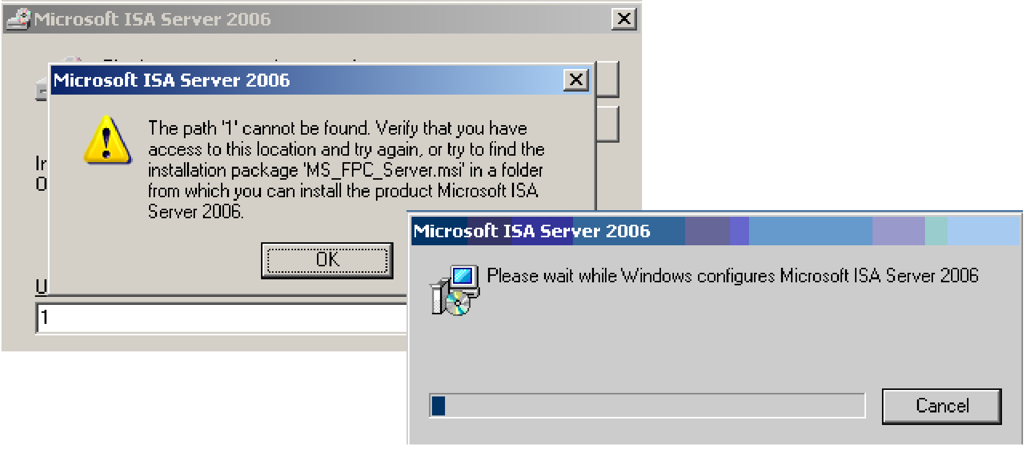
Click OK to accept this behavior and continue. Click Cancel to return to the page.

□ Don't tell me about this again.

Figure 3: Users retain ownership of objects they created

### Open the ISA Management console with no access

Another interesting thing is what happens when a user tries to open the ISA Server 2006 management console when the user has no assigned ISA Server 2006 roles. I tried it with the user Auditor who has no assigned ISA Server role. You can see the result in the following picture.



Microsoft ISA Server 2006

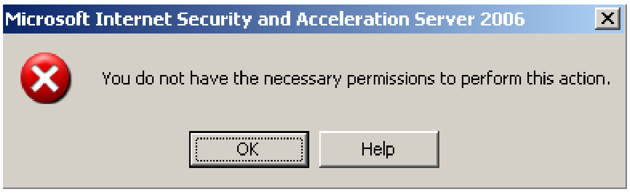
The path '1' cannot be found. Verify that you have access to this location and try again, or try to find the installation package 'MS_FPC_Server.msi' in a folder from which you can install the product Microsoft ISA Server 2006.

Please wait while Windows configures Microsoft ISA Server 2006

Figure 4: Messages when a user tries to open the ISA Management console without assigned roles

### Testing the ISA role concept

As a next step, I logged on with the user Auditor which I assigned the ISA Server Auditor rule. After the Management console has opened, I tried to create a new firewall rule but this should not have success, because the ISA Server Auditor rule should not have the right to create firewall rules.



Microsoft Internet Security and Acceleration Server 2006

You do not have the necessary permissions to perform this action.

Figure 5: The ISA Server Auditor rules doesn't have the permission to create a firewall rule

### Defining Enterprise-Level Administrative Roles

ISA Server 2006 Enterprise also uses a role-based model to organize enterprise and array administrators with predefined roles. Users with a specific role are allowed to complete specific ISA Server tasks. ISA Server 2006 distinguishes between enterprise-level roles and array level roles. ISA Server 2006 Enterprise can assign the following Enterprise:

| ISA Server 2006 Enterprise role | Tasks |
|---|---|
| ISA Server Enterprise Administrator | This role allows full control over the enterprise and the configuration of all arrays in the enterprise. Users with this role can create enterprise policies and apply them to an array, manage array configurations, and assign roles to other users and groups |
| ISA Server Enterprise Auditor | This role allows users to view the enterprise configuration and the configuration of all arrays in the enterprise |
| ISA Server Enterprise Policy Editor | Enterprise administrators can assign administrators permissions for specific enterprise policies, thus limiting |

| | |
|---|---|
| | enterprise-level administration to a specific policy. Enterprise Policy Editors can create rules for the specific enterprise policy, but cannot create new enterprise policies |

Table 3: ISA Server 2006 Enterprise roles

### Discretionary Access Control Lists

When ISA Server 2006 is installed, it uses discretionary access control lists (DACLs) to configure permission. ISA Server 2006 reconfigures the DACLs every time when the Microsoft ISA Server Control service (ISACTRL) is restarted or when you add new administrative ISA Server roles.

### Conclusion

In this article I tried to show you how to delegate administrative permissions for administering ISA Server 2006 with different users and user groups. Distributing the Firewall administration is often required in enterprise environments where many ISA Servers must be administered and administrative work is distributed through the admin staff.

In my opinion, delegating administrative permissions in ISA Server 2006 is extremely useful in ISA Server 2006 Enterprise, because of the array model and the enterprise environment it may be useful to separate the administrative permissions to administer ISA Server 2006.

### Related links

Role-based Administration in ISA Server 2006
http://technet.microsoft.com/en-us/library/bb794769.aspx
Enterprise Management in ISA Server 2006
http://www.microsoft.com/technet/isa/2006/enterprisemanagement.mspx
Security Guide
http://www.microsoft.com/technet/isa/2006/security_guide.mspx