

Installing ISA Server 2004 Enterprise Edition – Part III – Administering ISA Server 2004 Enterprise Arrays

Written by Marc Grote - <mailto:grotem@it-training-grote.de>

Abstract

This is the third part article of a four part article series which will show you how to manage ISA Server 2004 Enterprise Arrays. These article series will contain the following articles:

- Installing ISA Server 2004 Enterprise Edition – Part I – Installing and Configuring the Configuration Storage Server
- Installing ISA Server 2004 Enterprise Edition – Part II – Installing ISA Server 2004 Firewall on two Servers
- Administering ISA Server 2004 Enterprise Arrays
- Enabling CARP and NLB in ISA Server 2004 Enterprise

If you have more ideas about ISA Server 2004 Enterprise articles, please let me know and I will check if your idea could be part of a new article.

Let's begin

For this article series we have the following configuration:

Name	Role	Configuration
DEN-DC-01	Windows 2003 Domain Controller	INTERNAL: 192.168.1.10
DEN-CSS-01	Windows 2003 Member Server with ISA Server 2004 Configuration Storage Server	INTERNAL: 192.168.1.20
DEN-ISAE-01	Windows 2003 Member Server with ISA Server 2004 Enterprise Firewall	INTRAARRAY: 192.168.0.1 INTERNAL: 192.168.1.1 EXTERNAL: 172.16.1.1
DEN-ISAE-02	Windows 2003 Member Server with ISA Server 2004 Enterprise Firewall	INTRAARRAY: 192.168.0.2 INTERNAL: 192.168.1.2 EXTERNAL: 172.16.1.2

Role assignment at the Enterprise Level

With ISA Server 2004 Standard and Enterprise it is possible to assign different roles for delegation of administrative tasks to users or groups of users. This functionality has been enhanced in ISA Server 2004 Enterprise to delegate roles on Enterprise- and Array Level (**Figure 1**). You can delegate the following roles at the Enterprise Level:

- ISA Server Enterprise Administrator
- ISA Server Enterprise Auditor

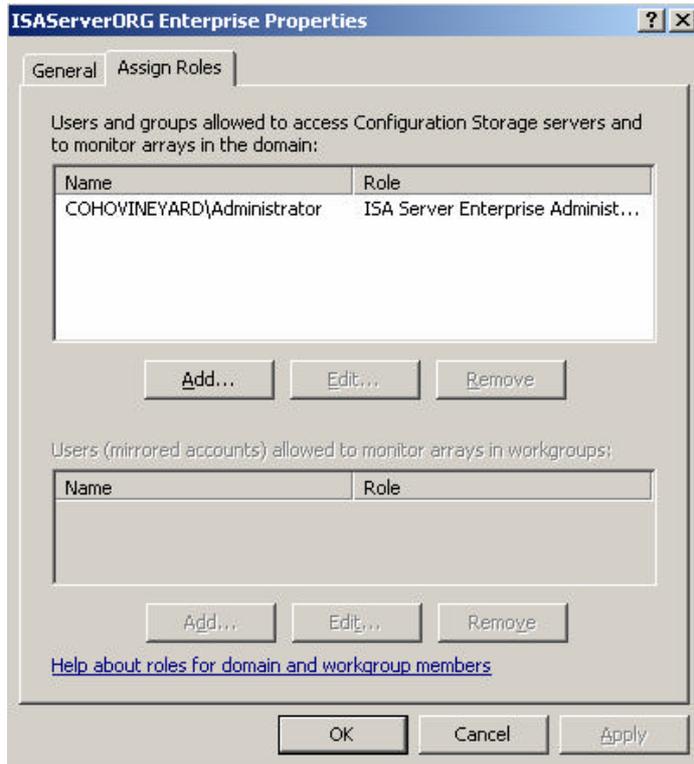


Figure 1: Delegation of roles at Enterprise Level

Click **Browse** to add a Group or User (**Figure 2**) and select the role for this user or group. The ISA Server Enterprise Administrator has all privileges to manage the Enterprise and all Arrays. The ISA Server Enterprise Auditor rule allows a user to display the whole ISA Server Enterprise and Array Level configuration without the right to make any configuration changes.

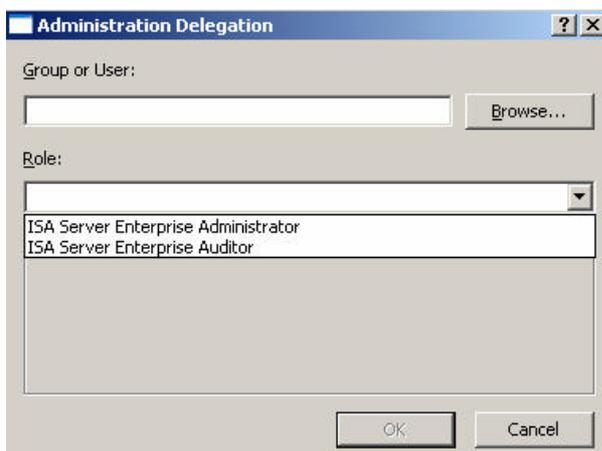


Figure 2: Select a User or Group for Role based Access

Role assignment at the Array Level

Like in ISA Server 2004 Standard it is possible to assign roles at the Array Level in ISA Server 2004 Enterprise. To assign a role right click the Array Properties and select **Assign Roles** and add the required Users or Group (**Figure 3**).



Figure 3: Assign Roles at Array Level

You can assign the following roles at the Array Level:

- ISA Server Array Monitoring Auditor
- ISA Server Array Auditor
- ISA Server Array Administrator

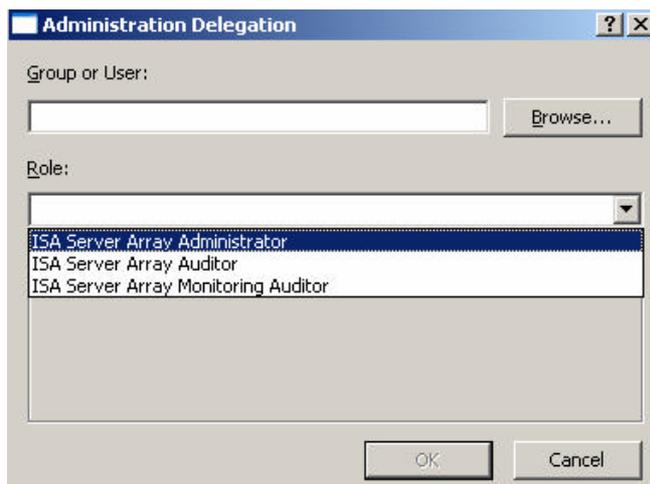


Figure 4: Select a User or Group for Role based Access at Array Level

ISA Server Array Monitoring Auditor

Users and groups assigned this role can monitor the ISA computer and network activity, but cannot configure specific monitoring functionality.

ISA Server Array Auditor

Users and groups assigned this role can perform all monitoring tasks.

ISA Server Array Administrator

Users and groups assigned this role can perform all ISA Server Management tasks.

Enterprise Policies

One of the new features of ISA Server 2004 Enterprise is the ability to create Enterprise Policies for the whole ISA Enterprise. The Enterprise Policy enhances centralized management introduced by arrays, allowing you to implement and apply policy to the arrays in your corporate network. The Enterprise Policy contains an ordered set of policy rules.

You can create one or more Enterprise Policies and a single set of Enterprise-Level rule elements. An ISA Enterprise Administrator can define several Enterprise Policies, such as an Enterprise Policy that allows the HTTP protocol for all protected networks.

Each rule in the Policy can be defined apply before or after the Array Policy. There is one default Enterprise Policy created during the installation of the first Configuration Storage Server. This Policy is named **Default** and denies all Traffic (**Figure 5**). The default enterprise policy cannot be modified or deleted.

When configuring an Enterprise Policy, you can order the Enterprise Rules, moving them so that they are processed before the Array Rules or after the Array Rules. Only the default rule cannot be reordered. It is always processed last.



Figure 5: Default Enterprise Policy

To create a new Enterprise Policy right click **Enterprise Policies – New – Enterprise Policy**. In our example we will name the new policy **ISAServerOrg**.

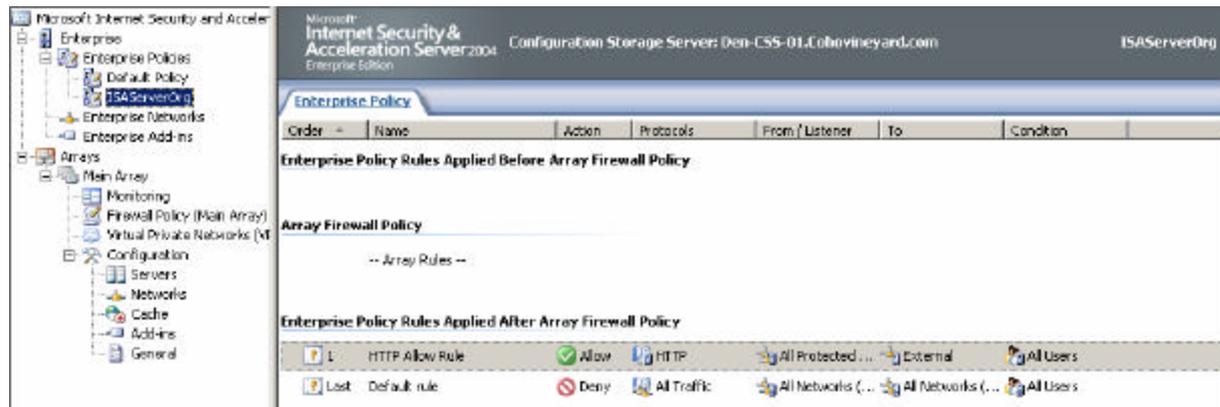


Figure 6: New Enterprise Policy

It is possible to order Enterprise Policies before or after Array Policies. The Order of Policies is important. To know more about the importance of Rule ordering, read the following article from Stefaan Pouseele:

http://www.isaserver.org/articles/ISA2004_AccessRules.html.

After changing the rule order click **Apply (Figure 7)** to save the changes.



Figure 7: Click Apply to save changes

After creating a new Enterprise Policy you can assign any Enterprise Policy at the Array Level. To change the Enterprise Policy at the Array Level, navigate to the Array and right click the Array and click **Policy Settings** and choose the new Enterprise Policy (**Figure 8**).

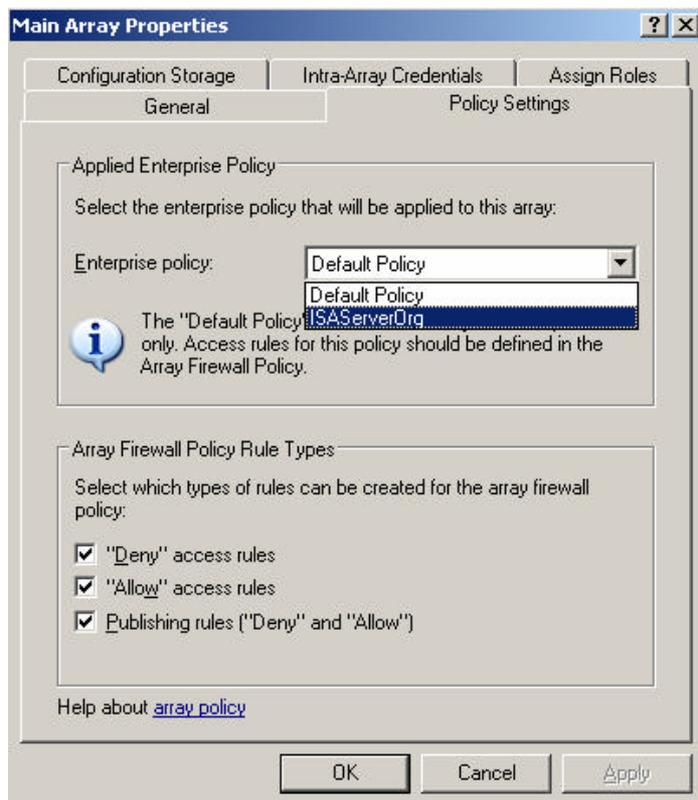


Figure 8: Assign Enterprise Policies to Arrays

Enterprise Networks

ISA Server 2004 Enterprise Networks represents all the IP addresses in your organization's network. An ISA Administrator can create Enterprise Networks which include IP address ranges from your Network Topology and use these Networks at Enterprise- or Array Level.

Using Enterprise Networks at the Enterprise level

You use Enterprise Networks to create Access rules at the Enterprise level. If you use these Networks in Firewall Policies, you can deploy these settings to multiple Arrays which use this Enterprise Policy. It is not possible to configure more settings in an Enterprise network like Webproxy, CARP and NLB settings. These settings are only possible at Array networks.

Using Enterprise Networks at the Array level

You can use Enterprise Networks at the Array level, by using them to define address ranges of Array-level networks. An Example: An Array Administrator can define an Array-level network called **DMZ**, and include the IP address range of the Enterprise Network **Enterprise-DMZ** in it.

Predefined Enterprise Networks

ISA Server 2004 includes predefined Enterprise Networks that act as placeholder objects for Array-level Networks with the same name. You cannot explicitly use Enterprise Networks in Array-level Firewall Policy rules. Instead, they are typically used in the enterprise policy. Any rule applied by the Enterprise Administrator to the

predefined Enterprise Network will be applied to the Array-level network of the same name. ISA Server 2004 uses the following predefined Enterprise Networks (**Figure 9**):

- External
- Local Host
- Quarantined VPN Clients
- VPN Clients



Figure 9: Enterprise networks

Choose Configuration Storage Servers

Right click the ISA Server Array click Configuration Storage and you will see the configured Configuration Storage Server. If you have more than one Configuration Storage Server you can enter the Alternate Configuration Storage Server name (**Figure 10**) into the field **Alternate Configuration Storage server (optional)**.

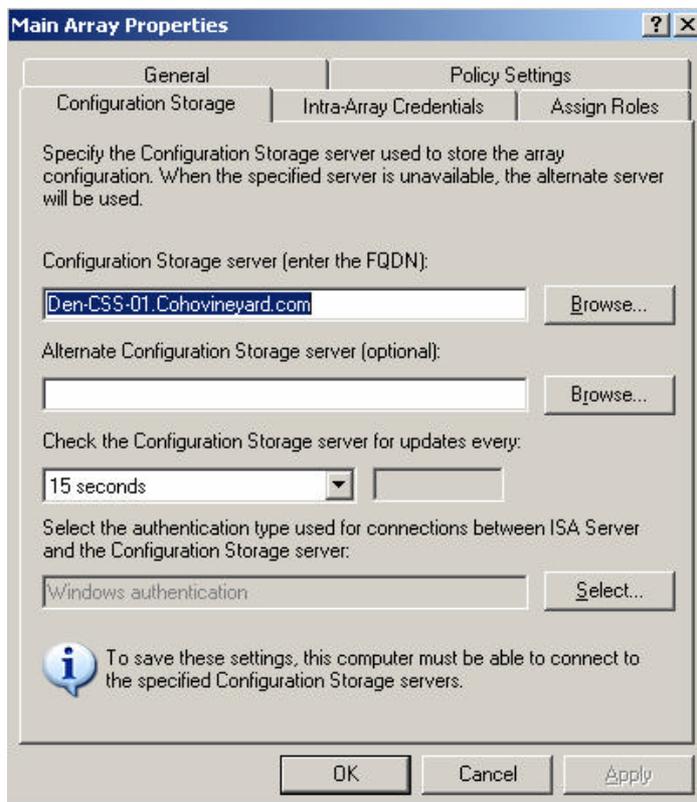


Figure 10: Choose the Configuration Storage Server

Copy Array Rule Elements

It is possible to copy selected Array Level Rule elements to the Enterprise Level. To do this, navigate to **Arrays – MainArray** – and right click **Copy Array Rule Elements** (Figure 11).

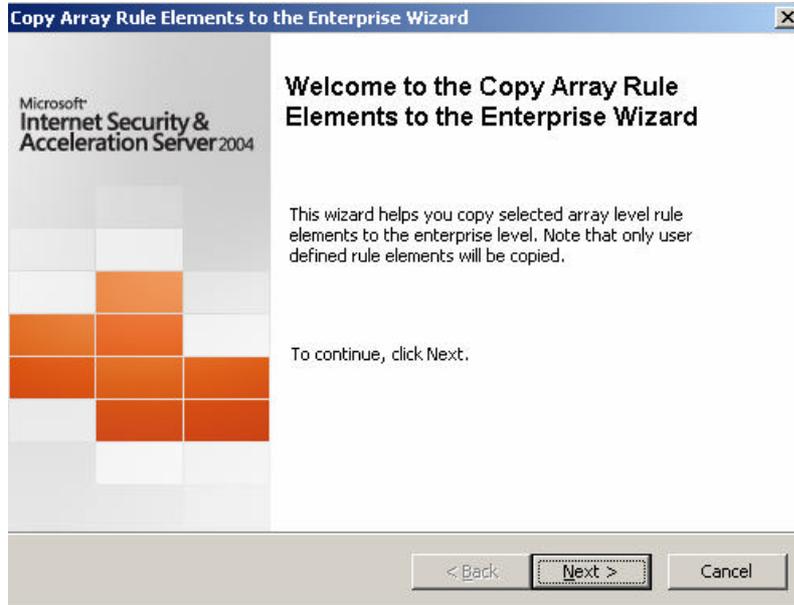


Figure 11: Copy Array Rule Wizard

Please note that it is only possible to copy user defined rule elements and not predefined objects.

Select the Array Rule Elements (Figure 12) that you would like to copy to the Enterprise Level.



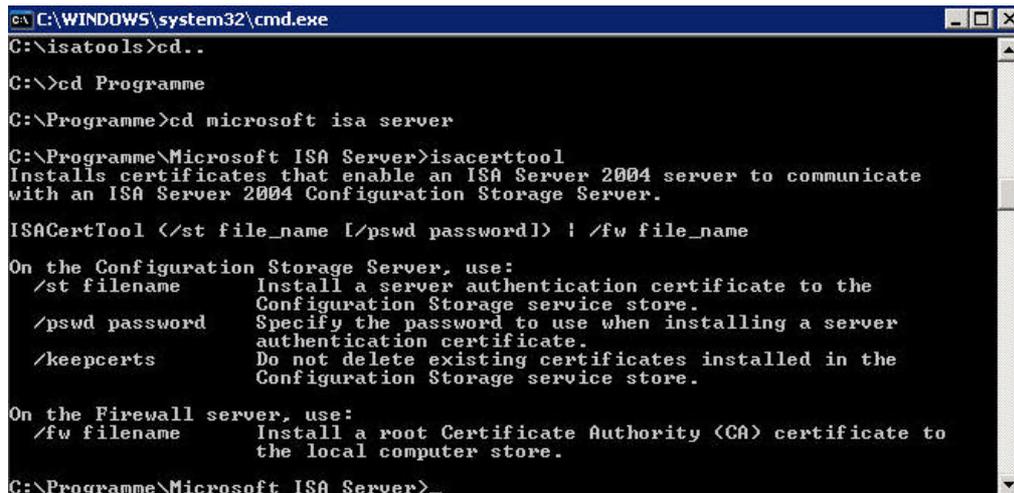
Figure 12: Select the Array Rule elements that should be copied

Click **Finish**.

ISACertTool

As you know, ISA Server 2004 Enterprise Edition uses a Configuration Storage Server (CSS) as storage for Enterprise and Array settings. When you use ISA Server in a workgroup scenario or in an environment with domains without trust relationships, you can use certificates to sign and seal the communication between ISA components. **ISACertTool (Figure 13)** is a handy tool if you want to change configuration settings after installation. **ISACertTool** helps you do the following:

- Install a Server Certificate on the Configuration Storage Server.
- Install a Root Certificate on each ISA Array Member



```
C:\WINDOWS\system32\cmd.exe
C:\isatools>cd..
C:\>cd Programme
C:\Programme>cd microsoft isa server
C:\Programme\Microsoft ISA Server>isacerttool
Installs certificates that enable an ISA Server 2004 server to communicate
with an ISA Server 2004 Configuration Storage Server.

ISACertTool </st file_name [/pswd password] ! /fw file_name

On the Configuration Storage Server, use:
  /st filename      Install a server authentication certificate to the
                    Configuration Storage service store.
  /pswd password   Specify the password to use when installing a server
                    authentication certificate.
  /keepcerts       Do not delete existing certificates installed in the
                    Configuration Storage service store.

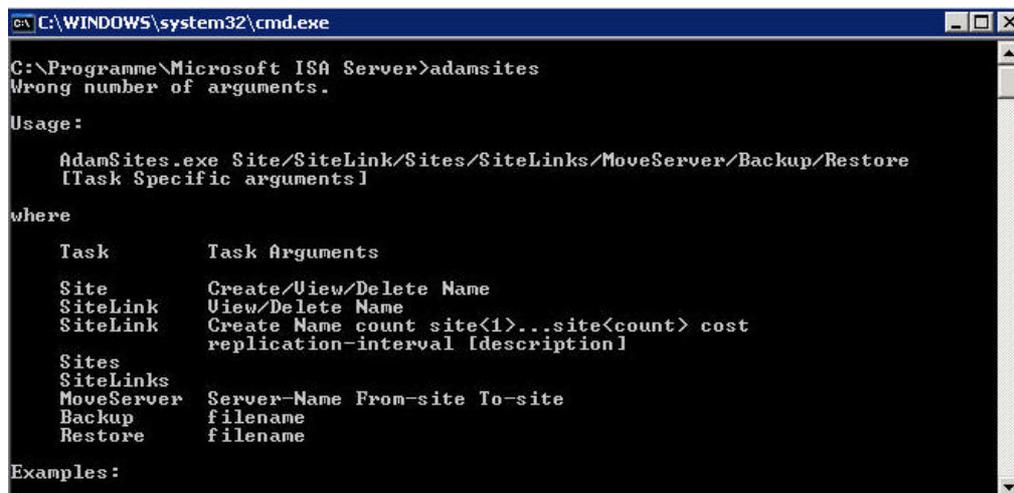
On the Firewall server, use:
  /fw filename      Install a root Certificate Authority (CA) certificate to
                    the local computer store.

C:\Programme\Microsoft ISA Server>
```

Figure 13: ISACertTool

ADAM Sites

ADAM uses the site concept like Windows Server 2003 Active Directory. When you deploy a Configuration Storage Server in your Organization, the ADAM instance will be created in Default First Site. If you deploy multiple Configuration Storage Servers, you can move Configuration Storage Servers to different sites or create SiteLinks and SiteLink costs (**Figure 14**) with the help of **ADAM Sites**.



```
C:\WINDOWS\system32\cmd.exe
C:\Programme\Microsoft ISA Server>adamsites
Wrong number of arguments.

Usage:

  AdamSites.exe Site/SiteLink/Sites/SiteLinks/MoveServer/Backup/Restore
  [Task Specific arguments]

where

  Task          Task Arguments
  Site          Create/View/Delete Name
  SiteLink      View/Delete Name
  SiteLink      Create Name count site<1>...site<count> cost
                replication-interval [description]
  Sites
  SiteLinks
  MoveServer    Server-Name From-site To-site
  Backup        filename
  Restore       filename

Examples:
```

Figure 14: ADAM Sites

Conclusion

In this article I have show you some aspects of ISA Server Enterprise configuration. The fourth article will show you how to implement ISA Server 2004 NLB and CARP within your enterprise.

Related Links

Deployment Guidelines for ISA Server 2004 Enterprise Edition

<http://www.microsoft.com/technet/prodtechnol/isa/2004/deploy/dgisaserver.aspx>

Introduction to Branch Deployment of ISA Server 2004 Enterprise Edition

http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/intro_to_branch_deployment_ee.aspx

ISA Server 2004 Enterprise Edition in a Workgroup

http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/workgroup_ee.aspx

Network Load Balancing in ISA Server 2004 Enterprise Edition

http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/network_load_balancing_ee.aspx

Troubleshooting Host IDs in ISA Server 2004 Enterprise Edition

<http://www.microsoft.com/technet/prodtechnol/isa/2004/hostid.aspx>

Troubleshooting Network Load Balancing in ISA Server 2004 Enterprise Edition

http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/ts_nlb_ee.aspx

ISA Server 2004 Enterprise Edition Configuration Guide

http://download.microsoft.com/download/6/9/0/690d2ee7-a4e0-4c0a-80d4-1e30ebcac1de/isa_2004_ee_configuration_guide.doc

Renaming Configuration Storage Servers in ISA Server 2004 Enterprise Edition

http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/renamecss_ee.aspx