Security Hardening Guide

Microsoft Internet Security and Acceleration Server 2004

Microsoft Corporation

Information in this document, including URL and other Internet Web site references, is subject to change without notice. The example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Contents

Introduction

This guide is designed to provide you with essential information about how to harden computers running Microsoft® Internet Security and Acceleration (ISA) Server 2004 Enterprise Edition or ISA Server 2004 Standard Edition. In addition to practical, specific configuration recommendations, this guide includes ISA Server deployment strategies.

For computers running Microsoft Windows Server™ 2003, this guide is a companion to the *Windows Server 2003 Security Guide*, located at the Microsoft TechNet Web site. Specifically, many of the procedures in this guide are related directly to security recommendations introduced in the *Windows Server 2003 Security Guide*. Therefore, before you perform the procedures presented in this guide, we recommend that you first read the *Windows Server 2003 Security Guide*.

If ISA Server is installed on a computer running Windows® 2000 Server, see the *Windows 2000 Server Hardening Guide* at the Microsoft Download Center.

Scope of This Guide

This guide focuses explicitly on the operations required to help create and maintain a secure ISA Server 2004 environment. You should use this guide as part of your overall security strategy for ISA Server 2004, and not as a complete reference for creating and maintaining a secure environment.

Specifically, this guide provides detailed answers to the following questions:

- What are the recommended steps for securing the ISA Server computer?
- What security considerations should be applied to the ISA Server configuration?
- What guidance is available to help prepare for a secure ISA Server 2004 deployment?

Securing the ISA Server Computer

An important step in securing ISA Server is verifying that the ISA Server computer is physically safe, and that you apply basic security configuration recommendations. Information about the following topics is provided:

- Managing updates
- Physical access
- Determining domain membership
- Hardening the Windows infrastructure
- Managing roles and permissions
- Reducing the attack surface

Lockdown mode

The following sections describe these issues and how to implement security recommendations.

Managing Updates

As a security best practice, we strongly recommend that you always install the latest updates for the operating system, for ISA Server, and for other components installed by ISA Server: Microsoft SQL Server™ 2000 Desktop Engine (MSDE 2000) and Office Web Components 2002 (OWC). Do the following:

Get operating system updates. Check Windows Update at the Microsoft Update Web site.

Get ISA Server updates. Check for the latest update information for downloads for ISA Server 2004 at the Microsoft Windows Server System Web site.

Search for the latest updates for MSDE 2000 and for OWC. For information, see *Microsoft Security Bulletin Search* at the Microsoft TechNet Web site.

We also recommend that you analyze system security periodically, using Microsoft Baseline Security Analyzer (MBSA). You can download MBSA at the Microsoft TechNet Web site.

Physical Access

Ensure that the ISA Server computer is stored in a physically secure location. Physical access to a server is a high security risk. Physical access to a server by an intruder could result in unauthorized access or modification, as well as installation of hardware or software designed to circumvent security. To maintain a secure environment, you must restrict physical access to the ISA Server computer.

If you suspect that the ISA Server computer was compromised, reinstall ISA Server.

Protecting Confidential Information in Case of Theft

For ISA Server Enterprise Edition, each array member contains encrypted, confidential information about the other array members. The array member also has the keys to decrypt the information.

For this reason, in case any array member is stolen, confidential information about the other array members is potentially at risk. In case of theft of any array member, modify all confidential information on all the other array members. Confidential information includes user credential passwords (for example, used for logging on to a computer running SQL Server), Remote Authentication Dial-In User Service (RADIUS) shared secrets, or preshared Internet Protocol security (IPsec) keys.

Determining Domain Membership

In many cases, you may want to set up the ISA Server computer as a member of a domain. For example, if you will create a policy that relies on domain user authentication, ISA Server should belong to a domain.

If the ISA Server computer is protecting the edge of your network, we recommend that you install it in a separate forest (rather than in the internal forest of your corporate network). You help protect the internal forest from being compromised, even if an attack is mounted on the forest of the ISA Server computer. To experience the administrative and security benefits of ISA Server as a domain member, we recommend that you deploy the ISA Server computer in a separate forest with a one-way trust to the corporate forest. (One-way trust is supported on Windows Server 2003 domains only.)

Note that when you install ISA Server as a domain member, you can lock down the ISA Server computer using Group Policy, rather than by configuring only a local policy.

For security reasons, if you do not require domain or Active Directory® directory service functionality for the ISA Server computer, consider installing the ISA Server computer in a workgroup. For example, if ISA Server is protecting the edge of the network, consider installing the computer in a workgroup.

Hardening the Windows Infrastructure

As previously mentioned, this guide assumes that you applied the configurations recommended in the *Windows Server 2003 Security Guide*. Specifically, you should apply the Microsoft Baseline Security Policy security template. However, do not implement the Internet Protocol security (IPsec) filters or any of the server role policies.

In addition, you should consider ISA Server functionality and harden the operating system accordingly.

> **Note**
>
> We recommend that you harden the Windows infrastructure after you have completely installed ISA Server. For ISA Server Enterprise Edition, install all the necessary Configuration Storage servers and the array members. Then, harden the computers.

Using the Security Configuration Wizard

The Microsoft Windows Server 2003 operating system with Service Pack 1 (SP1) includes an attack surface reduction tool called the Security Configuration Wizard (SCW). Depending on the server role you select, the SCW determines the minimum functionality required, and disables functionality that is not required.

When you install Windows Server 2003 SP1 on the ISA Server computer, you can install the SCW and use the wizard to harden the computer.

The SCW guides you through the process of creating, editing, applying, or rolling back a security policy based on the selected roles of the server. The security policies that are created with the SCW are .xml files that, when applied, configure services, network security, specific registry values, audit policy, and if applicable, Internet Information Services (IIS). The SCW includes a role for ISA Server computers.

To apply the appropriate ISA Server roles, perform the following steps

1. On the ISA Server computer, click **Start**, point to **Administrative Tools**, and then click **Security Configuration Wizard**.
2. In the Security Configuration Wizard, on the **Welcome** page, click **Next**.
3. On the **Configuration Action** page, select **Create a new security policy**.
4. On the **Select Server** page, in **Server**, type the name or IP address of the ISA Server computer.
5. On the **Processing Security Configuration Database** page, click **Next**.
6. On the **Welcome** page of the **Role-based Service Configuration** page, click **Next**.
7. On the **Select Server Roles** page, select the following, and then click **Next**:

Select **Microsoft Internet Security and Acceleration Server 2004**, if you are hardening a computer running the ISA Server services (for ISA Server Enterprise Edition, an array member).

Select **Remote Access/VPN Server**, if you will be using the ISA Server computer for virtual private network (VPN) functionality.

> **Note**
>
> Do not select any specific server roles when hardening a Configuration Storage server.

8. On the **Select Client Features** page, select the default client roles, as appropriate. No special client roles are specifically required for hardening ISA Server. Then, click **Next**.
9. On the **Select Administration and Other Options** page, select the following options:

Select **Microsoft Internet Security and Acceleration Server 2004 Enterprise Edition: Configuration Storage**, if the Configuration Storage server is installed on this computer (for ISA Server Enterprise Edition only).

Select **Microsoft Internet Security and Acceleration Server 2004 Enterprise Edition: Client installation share**, if the Firewall Client share is installed on this computer.

Select **Microsoft Internet Security and Acceleration Server 2004 Enterprise Edition: MSDE Logging**, if ISA Server advanced logging options are installed on this computer.

Select **Remote Access Quarantine Agent**, if you will enable quarantine for ISA Server. (You must have selected the **Remote Access/VPN Server** server role in step 7.)

10. On the **Select Additional Services** page, select the appropriate services and click **Next**.
11. Click **Next** until you finish the wizard.

For more technical guidance about the SCW, see *Security Configuration Wizard for Windows Server 2003* at the Microsoft Windows Server System Web site.

Hardening the Computer Manually

If Windows Server 2003 SP1 is not installed on the computer, you can configure the service startup mode, as described in this section. You configure the computer as the Security Configuration Wizard does.

Note that we recommend that you use the SCW to harden the computer, because it is best optimized to secure the ISA Server computer.

Core Services

The following table lists the core services that must be enabled for ISA Server and the ISA Server computer to function properly.

Service name	Rationale	Startup mode
COM+ Event System	Core operating system	Manual
Cryptographic Services	Core operating system (security)	Automatic
Event Log	Core operating system	Automatic
IPsec Services	Core operating system (security)	Automatic
Logical Disk Manager	Core operating system (disk management)	Automatic
Logical Disk Manager Administrative Service	Core operating system (disk management)	Manual
Microsoft Firewall	Required for normal functioning of ISA Server	Automatic
Microsoft ISA Server Control	Required for normal functioning of ISA Server	Automatic
Microsoft ISA Server Job Scheduler	Required for normal functioning of ISA Server	Automatic
Microsoft ISA Server Storage	Required for normal functioning of ISA Server	Automatic
MSSQL$MSFW	Required when MSDE logging is used for ISA Server	Automatic
Microsoft Distributed Transaction Coordinator (MS DTC)	Distributed Transaction Coordinator	Automatic
Network Connections	Core operating system (network infrastructure)	Manual
NTLM Security Support Provider	Core operating system (security)	Manual
Plug and Play	Core operating system	Automatic
Protected Storage	Core operating system (security)	Automatic
Remote Access Connection Manager	Required for normal functioning of ISA Server	Manual
Remote Procedure Call (RPC)	Core operating system	Automatic
Secondary Logon	Core operating system (security)	Automatic

Service name	Rationale	Startup mode
Security Accounts Manager	Core operating system	Automatic
Server	Required for ISA Server Firewall Client Share	Automatic
Smart Card	Core operating system (security)	Manual
SQLAgent$MSFW	Required when MSDE logging is used for ISA Server	Manual
System Event Notification	Core operating system	Automatic
Telephony	Required for normal functioning of ISA Server	Manual
Virtual Disk Service (VDS)	Core operating system (disk management)	Manual
Windows Management Instrumentation (WMI)	Core operating system (WMI)	Automatic
WMI Performance Adapter	Core operating system (WMI)	Manual

ISA Server Server Roles

The ISA Server computer may function in additional capacities, or roles, depending on how you use the computer. The following table lists possible server roles, describes when they may be required, and lists the services that should be activated when you enable the role.

Server role	Usage scenario	Services required	Startup mode
Remote Access/VPN Server	Users and groups assigned this role can monitor the ISA Server computer and network activity, but cannot configure specific monitoring functionality.	Routing and Remote Access	Manual
		Remote Access Connection Manager	Manual
		Telephony	Manual
		Workstation	Automatic
		Server	Automatic
Terminal Server	Select this role to enable remote management of the ISA Server computer.	Server	Automatic
		Terminal Services	Manual

Notes

The startup mode for the Server service should be Automatic in the following cases:

- You install ISA Server 2004: Client Installation Share.
- You use Routing and Remote Access Management, rather than ISA Server Management, to configure a virtual private network (VPN).
- Other tasks or roles, as described in the preceding table, require the service.

The startup mode for the Routing and Remote Access service is Manual. ISA Server starts the service only if a VPN is enabled.

Note that the Server service is required only if you use Routing and Remote Access Management (rather than ISA Server Management) to configure a VPN.

ISA Server Administration and Other Tasks

For a server to perform necessary tasks, specific services must be enabled, based on the roles that you select. Unnecessary services should be disabled. The following table lists possible server tasks for ISA Server, describes when they may be required, and lists the services that should be activated when you enable the role.

Server task	Usage scenario	Services required	Startup mode
Application Installation locally using Windows Installer	Required to install, uninstall, or repair applications using the Microsoft Installer Service.	Windows Installer	Manual
Backup	Required if using a backup program on the ISA Server computer.	Microsoft Software Shadow Copy Provider	Manual
		Volume Shadow Copy	Manual
		Removable Storage service	Manual
Error Reporting	Use to enable error reporting, thereby helping improve Windows reliability by reporting critical faults to Microsoft for analysis.	Error Reporting Service	Automatic
Help and Support	Allows collection of historical computer data for Microsoft Product Support Services incident escalation.	Help and Support	Automatic
ISA Server 2004: Client installation share	Required to allow computers to connect to and install from the Firewall Client share on the ISA Server computer.	Server	Automatic
ISA Server 2004: MSDE logging	Required to allow logging using MSDE databases. If you do not enable the applicable service, you can log to SQL databases or to files. However, you will not be able to use the log viewer in offline mode.	SQLAgent$MSFW	Manual
		MSSQL$MSFW	Automatic
Performance Data Collection	Allows background collecting of performance data on the ISA Server computer.	Performance Logs and Alerts	Automatic
Print	Allows printing from the ISA Server computer.	Print Spooler	Automatic
		TCP/IP NetBIOS Helper	Automatic

Server task	Usage scenario	Services required	Startup mode
		Workstation	Automatic
Remote Windows administration	Allows remote management of the Windows server (not required for remote management of ISA Server).	Server	Automatic
		Remote Registry	Automatic
Time Synchronization	Allows the ISA Server computer to contact an NTP server to synchronize its clock. From a security perspective, an accurate clock is important for event auditing and other security protocols.	Windows Time	Automatic
Remote Assistance Expert	Allows the Remote Assistance feature to be used on this computer.	Help and Support	Automatic
		Remote Desktop Help Session Manager	Manual
		Terminal Services	Manual

Notes

- To function properly, time client applications require that either the Wireless or the Server service is running.
- To function properly, performance counters require that both the Remote Registry and Server services are running.

ISA Server Client Roles

Servers can be clients of other servers. Client roles are dependent on role-specific services being enabled. The following table lists possible client roles for ISA Server, describes when they may be required, and lists the services that should be activated when you enable the role.

Client role	Usage scenario	Services required	Startup mode
Automatic Update client	Select this role to allow automatic detection and update from Microsoft Windows Update.	Automatic Updates	Automatic
		Background Intelligent Transfer Service	Manual
DHCP client	Select this role if the ISA Server computer receives its IP address automatically from a DHCP server.	DHCP Client	Automatic
DNS client	Select this role if the ISA Server computer needs to receive name resolution information from other servers. Also select the DNS Client role	DNS Client	Automatic

Client role	Usage scenario	Services required	Startup mode
	when ISA Server requires name resolution information (DNS and HOSTS file).		
Domain member	Select this role if the ISA Server computer belongs to a domain.	Network location awareness (NLA)	Manual
		Net logon	Automatic
		Windows Time	Automatic
DNS registration client	Select this role to allow the ISA Server computer to automatically register its name and address information with a DNS Server.	DHCP Client	Automatic
Microsoft Networking client	Select this role if the ISA Server computer has to connect to other Windows clients. If you do not select this role, the ISA Server computer will not be able to access shares on remote computers, for example, to publish reports.	TCP/IP NetBIOS Helper	Automatic
		Workstation	Automatic
WINS client	Select this role if the ISA Server computer uses WINS-based name resolution.	TCP/IP NetBIOS Helper	Automatic

Creating a Security Template

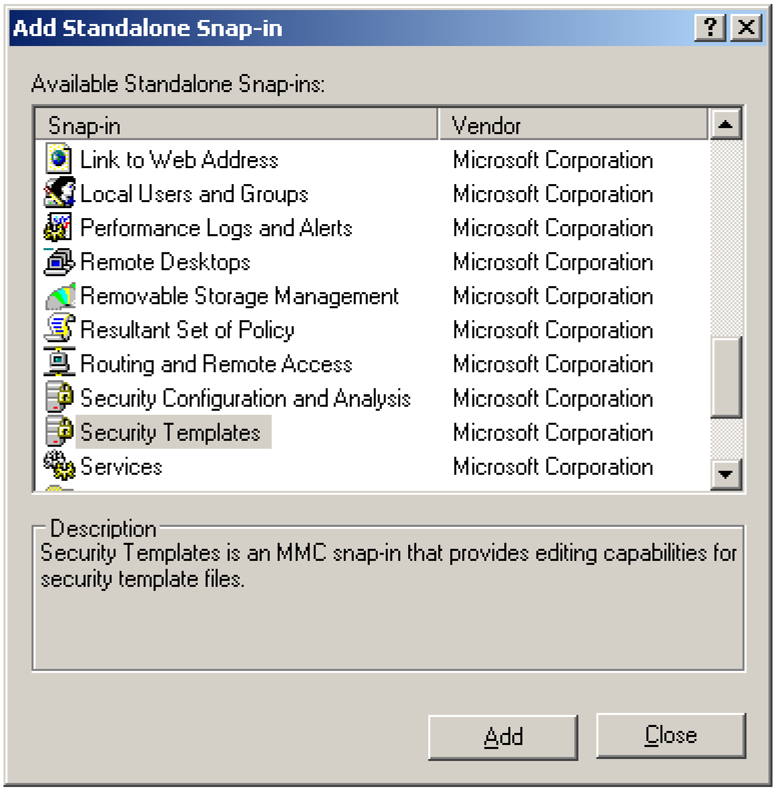
You can create a template, using the Security Templates Microsoft Management Console (MMC) snap-in. The template includes information about which services should be enabled, as well as their startup mode. By using a security template, you can easily configure a security policy and then apply it to each ISA Server computer.

To create a security template, perform the following steps

To open Security Templates, click **Start**, click **Run**, type **mmc**, and then click **OK**.

On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.

Select **Security Templates**, click **Add**, click **Close**, and then click **OK**.



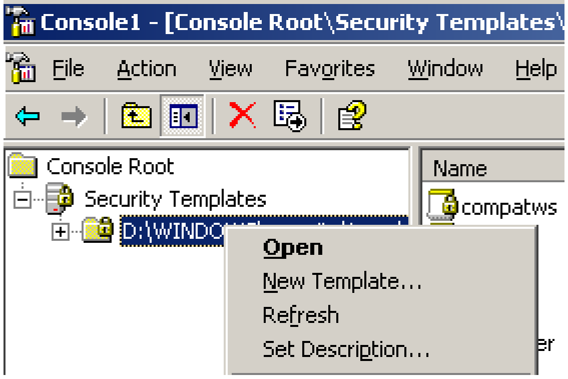
Available Standalone Snap-ins:

Snap-in	Vendor
Link to Web Address	Microsoft Corporation
Local Users and Groups	Microsoft Corporation
Performance Logs and Alerts	Microsoft Corporation
Remote Desktops	Microsoft Corporation
Removable Storage Management	Microsoft Corporation
Resultant Set of Policy	Microsoft Corporation
Routing and Remote Access	Microsoft Corporation
Security Configuration and Analysis	Microsoft Corporation
Security Templates	Microsoft Corporation
Services	Microsoft Corporation

Description

Security Templates is an MMC snap-in that provides editing capabilities for security template files.

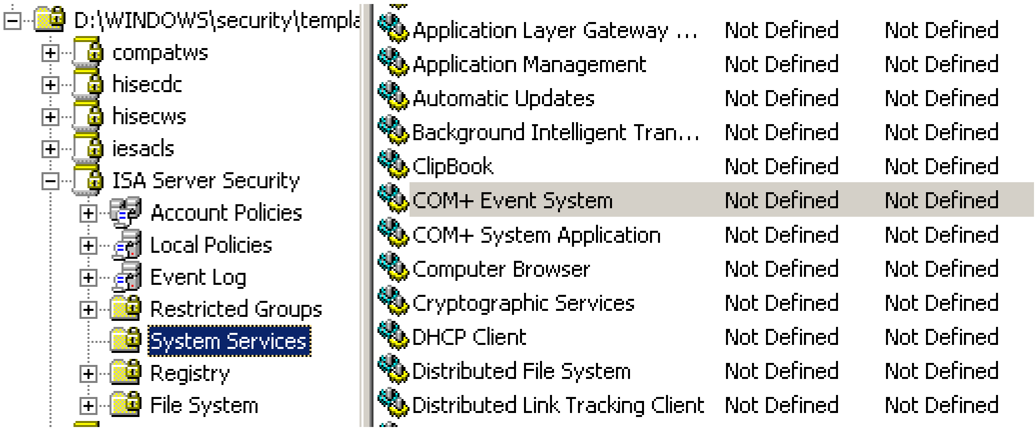
In the console tree, click the **Security Templates** node, right-click the folder where you want to store the new template, and click **New Template**.



In **Template name**, type the name for your new security template.

In **Description**, type a description of your new security template, and then click **OK**.

Expand the new template, and then click **System Services**.

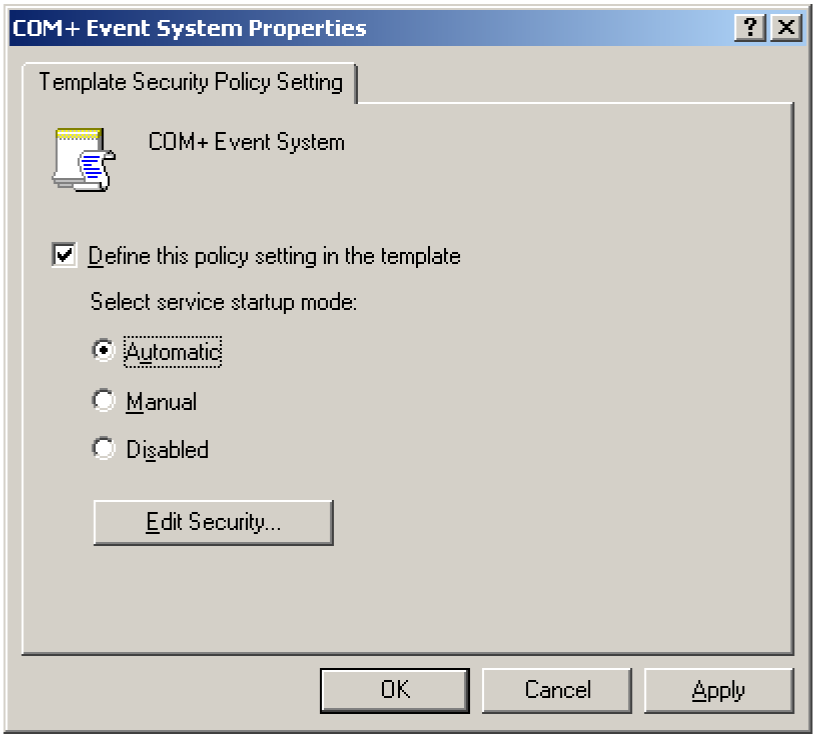


- D:\WINDOWS\security\templa
  - compatws
  - hisecdc
  - hisecws
  - iesacls
  - ISA Server Security
    - Account Policies
    - Local Policies
    - Event Log
    - Restricted Groups
    - System Services
    - Registry
    - File System

Application Layer Gateway ...	Not Defined	Not Defined
Application Management	Not Defined	Not Defined
Automatic Updates	Not Defined	Not Defined
Background Intelligent Tran...	Not Defined	Not Defined
ClipBook	Not Defined	Not Defined
COM+ Event System	Not Defined	Not Defined
COM+ System Application	Not Defined	Not Defined
Computer Browser	Not Defined	Not Defined
Cryptographic Services	Not Defined	Not Defined
DHCP Client	Not Defined	Not Defined
Distributed File System	Not Defined	Not Defined
Distributed Link Tracking Client	Not Defined	Not Defined

In the details pane, right-click **COM+ Event System**, and then click **Properties**.

Select **Define this policy setting in the template**, and then select the startup mode. (For COM+ Event System, the startup mode is **Automatic**.)



COM+ Event System Properties

Template Security Policy Setting

COM+ Event System

☑ Define this policy setting in the template

Select service startup mode:

● Automatic

○ Manual

○ Disabled

Repeat step 8 and step 9 for each of the services listed in the following table.

Service name	Short name	Startup mode
Automatic Updates	wuauserv	Automatic

Service name	Short name	Startup mode
Background Intelligent Transfer Service	BITS	Manual
COM+ Event System	EventSystem	Manual
Cryptographic Services	CryptSvc	Automatic
DHCP Client	Dhcp	Automatic
DNS Client	Dnscache	Automatic
Error Reporting Service	ERSvc	Automatic
Event Log	Eventlog	Automatic
Help and Support	Helpsvc	Automatic
IPsec Services	PolicyAgent	Automatic
Logical Disk Manager	dmserver	Automatic
Logical Disk Manager Administrative Service	dmadmin	Manual
Microsoft Firewall	Fwsrv	Automatic
Microsoft ISA Server Control	ISACtrl	Automatic
Microsoft ISA Server Job Scheduler	ISASched	Automatic
Microsoft ISA Server Storage	ISASTG	Automatic
Microsoft Software Shadow Copy Provider	SWPRV	Manual
MSSQL$MSFW	MSSQL$MSFW	Automatic
Network Connections	Netman	Manual
Network Location Awareness (NLA)	NLA	Manual
NTLM Security Support Provider	NtLmSsp	Manual
Performance Logs and Alerts	SysmonLog	Automatic
Plug and Play	PlugPlay	Automatic
Protected Storage	ProtectedStorage	Automatic
Remote Access Connection Manager	RasMan	Manual
Remote Desktop Help Session Manager	RDSessMgr	Manual
Remote Procedure Call (RPC)	RpcSs	Automatic
Removable Storage	NtmsSvc	Manual
Routing and Remote Access	None	Manual
Secondary Logon	seclogon	Automatic
Security Accounts Manager	SamSs	Automatic

Service name	Short name	Startup mode
Server	lanmanserver	Manual
Smart Card	SCardSvr	Manual
System Event Notification	SENS	Automatic
TCP/IP NetBIOS Helper	LmHosts	Automatic
Telephony	TapiSrv	Manual
Terminal Services	TermService	Manual
Virtual Disk Service (VDS)	VDS	Manual
Volume Shadow Copy	VSS	Manual
Windows Installer	MSIServer	Manual
Windows Management Instrumentation	winmgmt	Automatic
Windows Time	W32time	Automatic
Wireless Configuration	WZCSVC	Automatic
WMI Performance Adapter	WmiApSrv	Manual
Workstation	lanmanworkstation	Automatic

Notes

The startup mode for the Server service should be Automatic in the following cases:

- You install ISA Server 2004: Client Installation Share.
- You use Routing and Remote Access Management, rather than ISA Server Management, to configure a VPN.
- Other tasks or roles, as described in the preceding table, require the service.

The startup mode for the Routing and Remote Access service is Manual. ISA Server starts the service only if a VPN is enabled.

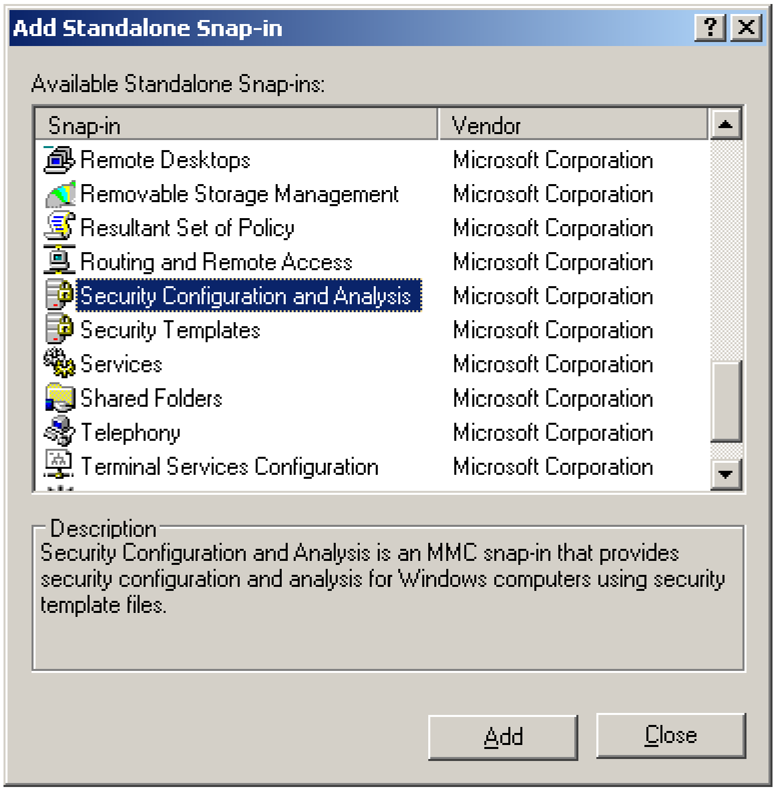
To function properly, time client applications require that either the Wireless or the Server service is running.

To apply the new template to the ISA Server computer, perform the following steps

To open Security Templates, click **Start**, click **Run**, type **mmc**, and then click **OK**.

On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.

Select **Security Configuration and Analysis**, click **Add**, click **Close**, and then click **OK**.



Available Standalone Snap-ins:

Snap-in	Vendor
Remote Desktops	Microsoft Corporation
Removable Storage Management	Microsoft Corporation
Resultant Set of Policy	Microsoft Corporation
Routing and Remote Access	Microsoft Corporation
Security Configuration and Analysis	Microsoft Corporation
Security Templates	Microsoft Corporation
Services	Microsoft Corporation
Shared Folders	Microsoft Corporation
Telephony	Microsoft Corporation
Terminal Services Configuration	Microsoft Corporation

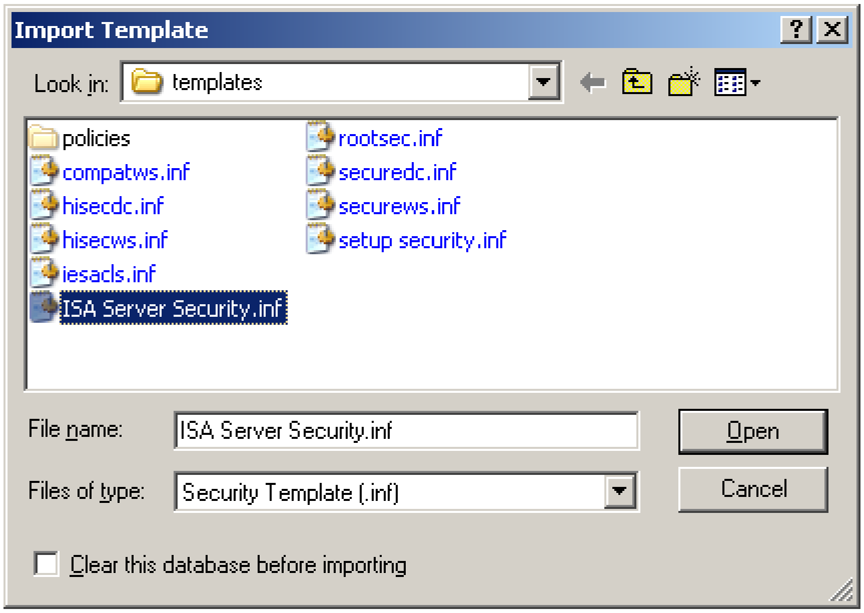
Description
Security Configuration and Analysis is an MMC snap-in that provides security configuration and analysis for Windows computers using security template files.

In the console tree, click **Security Configuration and Analysis**.

Right-click **Security Configuration and Analysis**, and then click **Open Database**.

Type a new database name, and then click **Open**.

Select a security template to import, and then click **Open**. Select the security template that you created previously.



Look in: templates

File name: ISA Server Security.inf

Files of type: Security Template (.inf)

☐ Clear this database before importing

Right-click **Security Configuration and Analysis**, and then click **Configure Computer Now.**

Managing Roles and Permissions

Because ISA Server controls access to your network, you should take special care in assigning permissions to the ISA Server computer and related components. Carefully determine who should have permission to log on to the ISA Server computer. Then, configure the logon rights accordingly.

ISA Server allows you to apply administrative roles to users and groups. After you determine which groups are allowed to configure or view ISA Server policy and monitoring information, you can assign roles appropriately.

The following sections detail considerations when assigning administrative roles and permissions.

Administrative Roles

As with any application in your environment, when you define the permissions for ISA Server, you should consider the roles of your ISA Server administrators and assign them only the necessary permissions. To simplify the process, ISA Server uses administrative roles. You can use role-based administration to organize your ISA Server administrators into separate, predefined roles, each with its own set of tasks. When you assign a role to a user, you essentially allow that user permissions to perform specific tasks. A user that has one role, such as ISA Server Full Administrator, can perform specific ISA Server tasks that a user with another role, such as ISA Server Basic Monitoring, cannot perform. Role-based administration involves

Windows users and groups. These security permissions, group memberships, and user rights are used to distinguish which users have which roles. The following table describes the ISA Server Standard Edition roles.

Standard Edition role	Description
ISA Server Basic Monitoring	Users and groups assigned this role can monitor the ISA Server computer and network activity, but cannot configure specific monitoring functionality.
ISA Server Extended Monitoring	Users and groups assigned this role can perform all monitoring tasks, including log configuration, alert definition configuration, and all monitoring functions available to the ISA Server Basic Monitoring role.
ISA Server Full Administrator	Users and groups assigned this role can perform any ISA Server task, including rule configuration, applying of network templates, and monitoring.

The following table describes the ISA Server Enterprise Edition roles.

Enterprise Edition role	Description
ISA Server Array Monitoring Auditor	Users and groups assigned this role can monitor the ISA Server 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, including log configuration, alert definition configuration, and all monitoring functions available to the ISA Server Basic Monitoring role in Standard Edition.
ISA Server Array Administrator	Users and groups assigned this role can perform any ISA Server task, including rule configuration, applying of network templates, and monitoring.
ISA Server Enterprise Administrator	Users and groups assigned this role have full control over the enterprise and all array configurations. The Enterprise Administrator can also assign roles to other users and groups.
ISA Server Enterprise Auditor	Users and groups assigned this role can view the enterprise configuration and all array configurations.

Members of these ISA Server administrative groups can be any Windows user. No special privileges or Windows permissions are required. The only exception is that to view the ISA Server performance counters, using perfmon or the ISA Server Dashboard, the user must be a member of the Windows Server 2003 Performance Monitor Users group.

Note that administrators with ISA Server Extended Monitoring permissions can export and import all configuration information, including secret configuration information. This means that they can decrypt secret information.

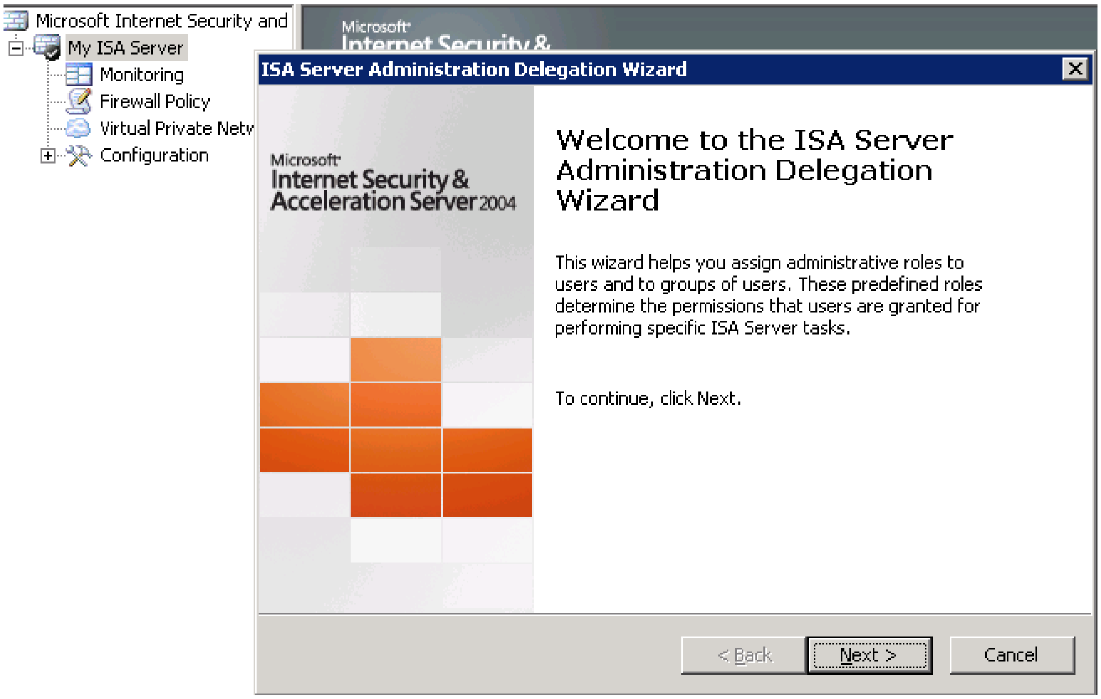
Users with administrator permissions on the ISA Server computer do not automatically have ISA Server array-level permissions or enterprise-level permissions. You must specifically assign these users the appropriate roles. Note, however, that users that belong to the Administrators group on the Configuration Storage server can essentially control the enterprise configuration. This is because they can directly modify any data on the Configuration Storage server.

To assign administrative roles for ISA Server Standard Edition, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Microsoft Internet Security and Acceleration Server 2004** and then click ***Server_Name***.

On the **Tasks** tab, click **Define Administrative Roles**.


Microsoft Internet Security and
My ISA Server
Monitoring
Firewall Policy
Virtual Private Netw
Configuration
Microsoft Internet Security &
Microsoft Internet Security & Acceleration Server 2004
< Back
Next >
Cancel

ISA Server Administration Delegation Wizard

Welcome to the ISA Server Administration Delegation Wizard

This wizard helps you assign administrative roles to users and to groups of users. These predefined roles determine the permissions that users are granted for performing specific ISA Server tasks.

To continue, click Next.

On the **Welcome** page of the ISA Server Administration Delegation Wizard, click **Next**.

Click **Add**.

In **Group (recommended) or User**, type the name of the group or user to which the specific administrative permissions will be assigned.

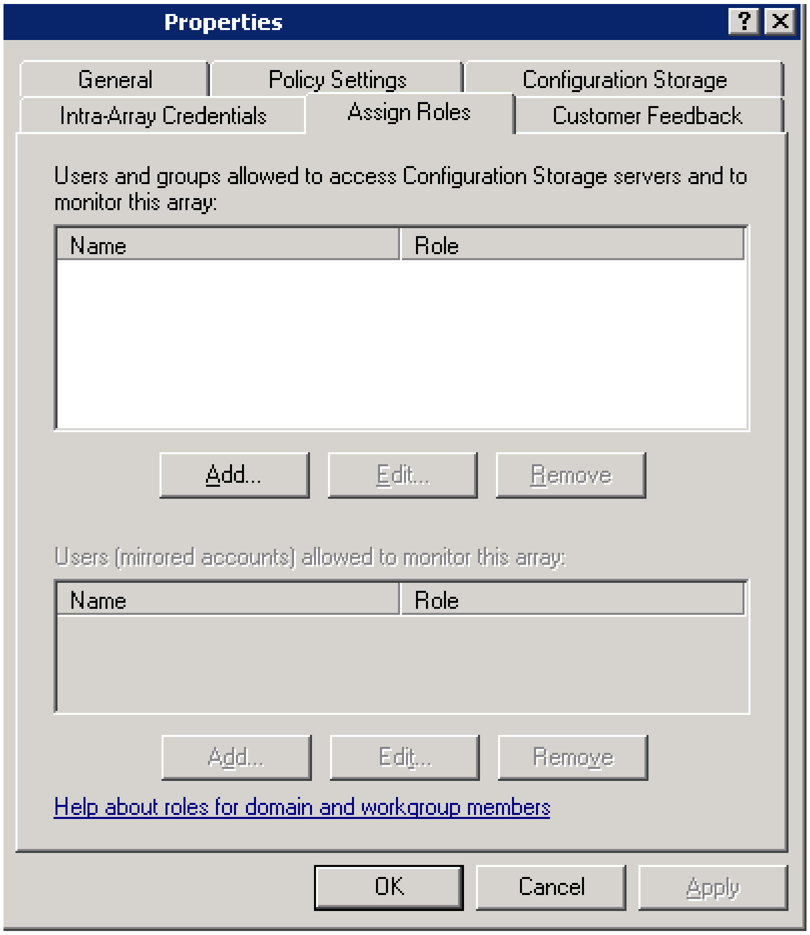
In **Role**, select the applicable administrative role.

To assign administrative roles for ISA Server Enterprise Edition, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Virtual Private Networks (VPN)**.

On the **Tasks** tab, click **Assign Administrative Roles**.

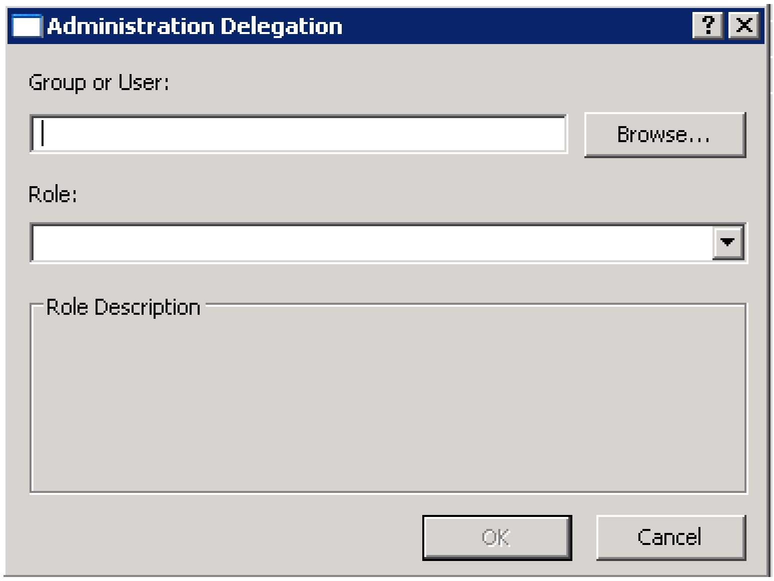


Users and groups allowed to access Configuration Storage servers and to monitor this array:

Users (mirrored accounts) allowed to monitor this array:

If the computer running the ISA Server services is in a domain, on the **Assign Roles** tab, click the upper **Add** button. Then, in **Group or User**, type the name of the group or user that can access the Configuration Storage server. In **Role**, select one of the following:

- **ISA Server Array Administrator**. Allows the specified group or user full control permissions for the array. The administrator can also view the enterprise policy applied to the array.
- **ISA Server Array Auditor**. Allows the specified group or user monitoring permissions and to view the array configuration.
- **ISA Server Array Monitoring Auditor**. Allows the specified group or user some monitoring permissions.



If the computer running the ISA Server services is in a workgroup, on the Assign Roles tab, click the lower Add button. Then, in **Group or User**, type the name of the group or user that can access the Configuration Storage server. In **Role**, select one of the following:

- **ISA Server Array Administrator**. Allows the specified group or user full control permissions for the array. The administrator can also view the enterprise policy applied to the array.
- **ISA Server Array Auditor**. Allows the specified group or user monitoring permissions and to view the array configuration.
- **ISA Server Array Monitoring Auditor**. Allows the specified group or user some monitoring permissions.

Credentials

When requested to present credentials, use strong passwords. A password is considered strong if it provides an effective defense against unauthorized access. A strong password does not contain all or part of the user account name, and contains at least three of the four following categories of characters: uppercase characters, lowercase characters, base 10 digits, and symbols found on the keyboard (such as !, @, or #).

Permissions

Apply the principle of least privilege when configuring permissions for ISA Server administrators, as described in the following section. Carefully determine who is allowed to log on to the ISA Server computer, eliminating access to those who are not critical to the server's functioning.

Least Privileges

Apply the principle of least privilege, where a user has the minimum privileges necessary to perform a specific task. This helps ensure that, if a user account is compromised, the impact is minimized by the limited privileges held by that user.

Keep the Administrators group and other user groups as small as possible. A user who belongs to the Administrators group on the ISA Server computer, for example, can perform any task on the ISA Server computer.

In Standard Edition, users in the Administrators group are implicitly assigned the role of ISA Server Full Administrator. They have full rights to configure and monitor ISA Server. For more information about roles, see the Administrative Roles section.

In Enterprise Edition, users who belong to the Administrators group on the Configuration Storage server can control the enterprise configuration. They can directly modify any data on the Configuration Storage server.

Logging On and Configuring

When you log on to the ISA Server computer, log on with the least privileged account necessary to do the task. For example, to configure a rule, you should log on as an ISA Server administrator. However, if you only want to view a report, log on with lesser privileges.

In general, use an account with restrictive permissions to perform routine tasks that are unrelated to administration, and use an account with broader permissions only when performing specific administrative tasks.

Guest Accounts

We recommend that you do not enable the Guest account on the ISA Server computer.

When a user logs on to the ISA Server computer, the operating system checks whether the credentials match a known user. If the credentials do not match a known user, the user is logged on as Guest, with the same privileges allowed to the Guest account.

ISA Server recognizes the Guest account as the default All Authenticated Users user set.

Discretionary Access Control Lists

With a new installation, ISA Server discretionary access control lists (DACLs) are appropriately configured. In addition, ISA Server reconfigures DACLs appropriately when you modify administrative roles (for more information, see the Administrative Roles section) and when the ISA Server Control Service (isactrl) is restarted.

Warning

Because ISA Server periodically reconfigures DACLs, you should not use the Security and Configuration Analysis tool to configure the per-file DACLs on the ISA Server objects. Otherwise, there may be a conflict between the DACLs set by Group Policy and the DACLs that ISA Server tries to configure.

Do not modify the DACLs set by ISA Server. Note that ISA Server does not set DACLs for the objects in the following list. You should set DACLs for the objects in the following list carefully, giving permissions only to trusted, specific users:

Folder for reports (when you select to publish the reports).

Configuration files created when exporting or backing up the configuration.

Log files that are backed up to a different location.

Be sure to carefully set DACLs, giving permissions only to trusted users and groups. Also, be sure to create strict DACLs on objects that are indirectly used by ISA Server. For example, when creating an ODBC connection that will be used by ISA Server, be sure to keep the Data Source Name (DSN) secure.

Configure strict DACLs for all applications running on the ISA Server computer. Be sure to configure strict DACLs for associated data in the file system and in the registry.

If you customize the SecurID HTML or error message templates, be sure to configure appropriate DACLs. The recommended DACL is "Inherit permission from parent."

Tip

We recommend that you do not save critical data (such as executables and log files) to FAT32 partitions. This is because DACLs cannot be configured for FAT32 partitions.

Revoking User Permissions

When you revoke administrative permissions for an ISA Server administrator, be sure to also perform the following:

On the ISA Server computer, delete the user's account.

On the Configuration Storage server (for ISA Server Enterprise Edition), review the Active Directory Application Mode (ADAM) objects. Modify the ownership of objects that belong to the revoked account.

Modify the ownership of objects that belong to the revoked account.

Reducing the Attack Surface

To further secure the ISA Server computer, apply the principle of *reduced attack surface*. To reduce the breadth of your attack surface, follow these guidelines:

Do not run unnecessary applications and services on the ISA Server computer. Disable services and functions not critical to the current task, as described in the Hardening the Windows Infrastructure section.

Disable ISA Server features that you do not use. For example, if you do not require caching, disable caching. If you do not require the VPN functionality of ISA Server, disable VPN client access.

Identify those services and tasks not critical to how you manage your network, and then disable the associated system policy rules.

Limit the applicability of the system policy rules to required network entities only. For example, the Active Directory system policy configuration group, enabled by default, applies to all computers on the Internal network. You could limit this to apply only to a specific Active Directory group on the Internal network.

The following sections describe how you can reduce the attack surface of the ISA Server computer.

Disabling ISA Server Features

Depending on your specific networking needs, you may not require the rich set of features included with ISA Server. You should carefully consider your specific needs, and determine whether you need the following:

VPN client access

Caching

Add-ins

If you do not require a specific feature, disable that feature.

VPN Client Access

VPN client access is disabled by default. This means that the relevant system policy rule, named Allow VPN client traffic to ISA Server, is also disabled. The default network rule, named VPN Clients to Internal Network, is enabled, even when VPN client access is disabled. If VPN client access had been previously enabled, you can disable it, if it is not required.

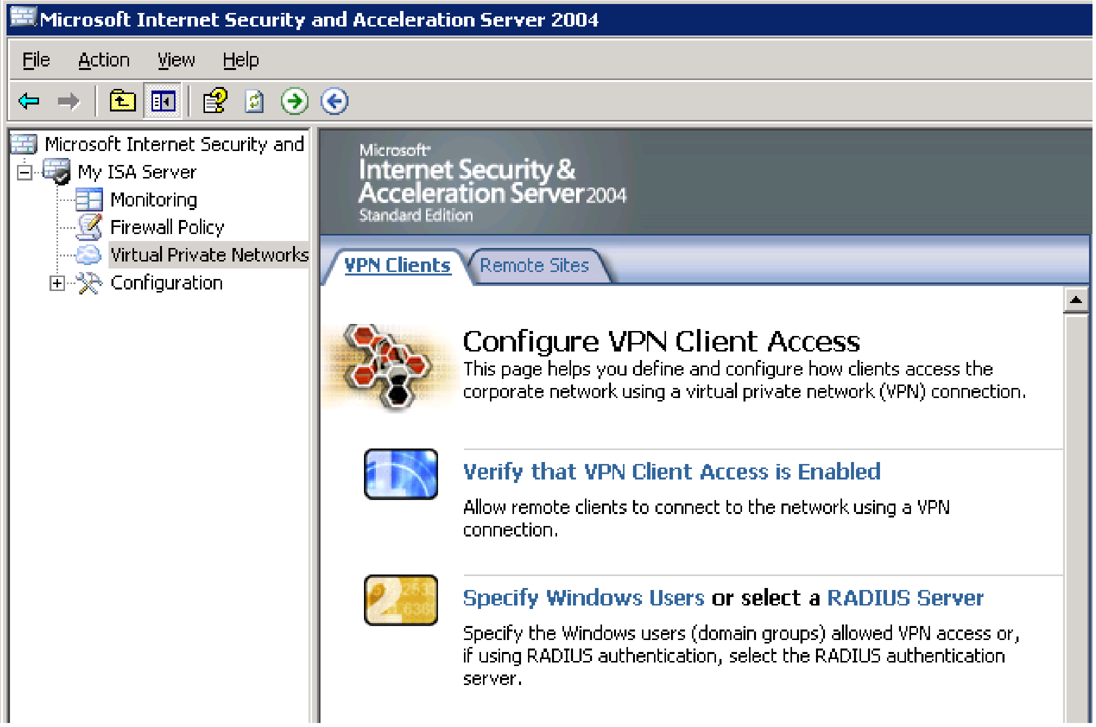
To verify that VPN client access is disabled, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Virtual Private Networks (VPN)**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Virtual Private Networks (VPN)**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Virtual Private Networks (VPN)**.

In the details pane, click the **VPN Clients** tab, and then click **Verify that VPN Client Access is Enabled**.



Configure VPN Client Access

This page helps you define and configure how clients access the corporate network using a virtual private network (VPN) connection.

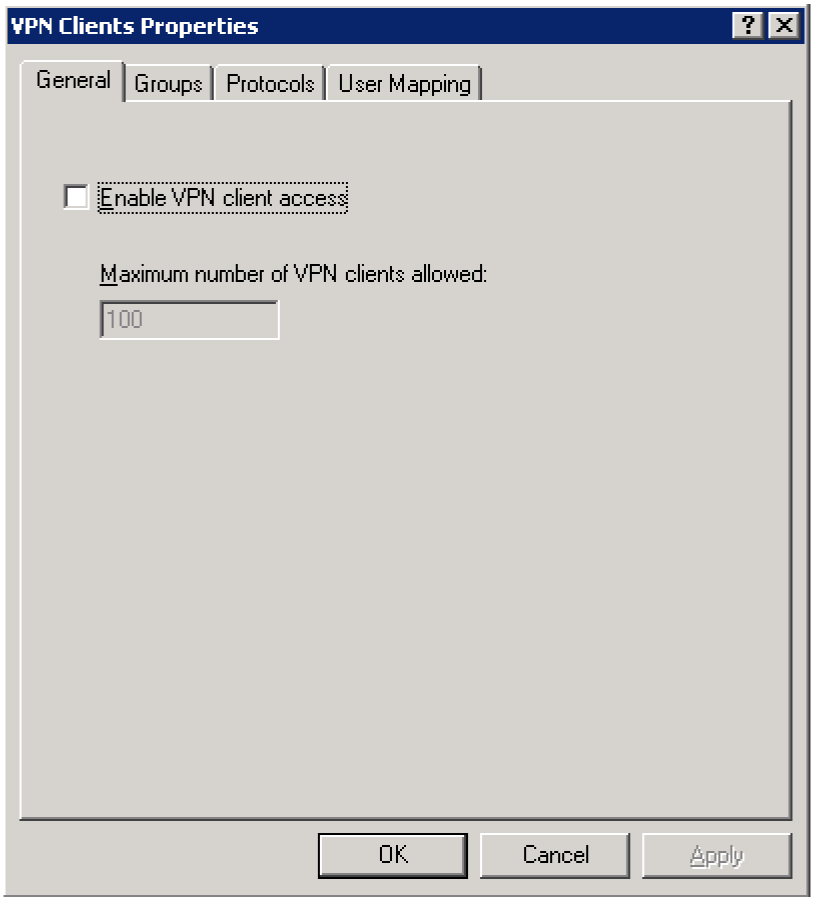
Verify that VPN Client Access is Enabled

Allow remote clients to connect to the network using a VPN connection.

Specify Windows Users or select a RADIUS Server

Specify the Windows users (domain groups) allowed VPN access or, if using RADIUS authentication, select the RADIUS authentication server.

On the **General** tab, verify that **Enable VPN client access** is not selected.



☐ Enable VPN client access

Maximum number of VPN clients allowed:

100

Caching

Caching is disabled by default. This means that all relevant caching features, including scheduled content download, are disabled. If caching was previously enabled for ISA Server, you can disable it.

To verify that caching is disabled, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Cache**:

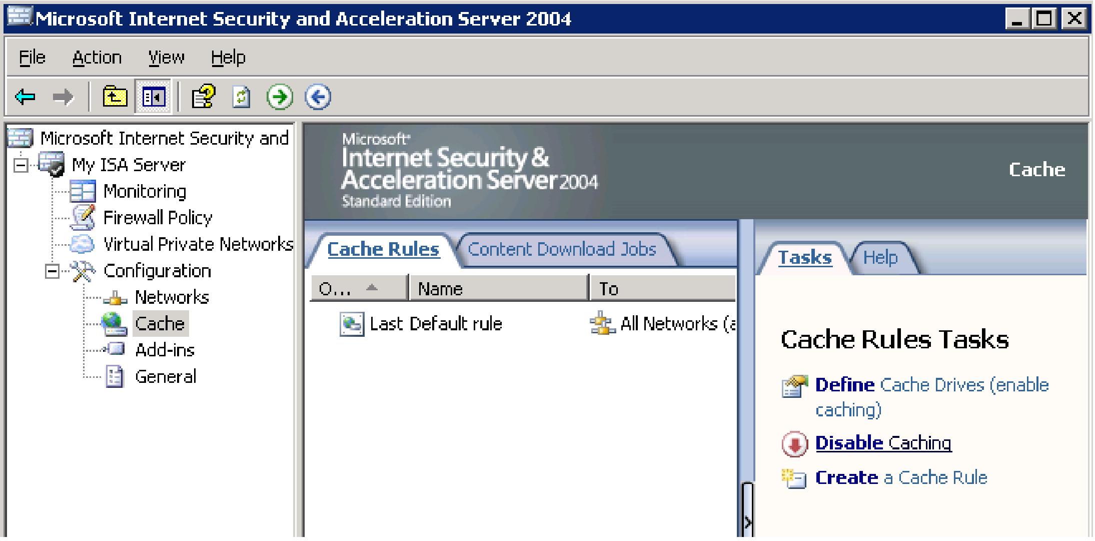
- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, expand **Configuration**, and then click **Cache**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, expand **Configuration**, and then click **Cache**.

In the details pane, for Enterprise Edition, click the **Cache Drives** tab. For Standard Edition, click the **Cache Rules** tab.

On the **Tasks** tab, click **Disable caching.**

Note

If caching is disabled, you will not see the option.



Add-ins

When you install ISA Server, a suite of application filters and Web filters are also installed. You can subsequently install additional add-ins, provided by third-party vendors. Follow these security guidelines:

Do not install application filters or Web filters that you do not require.

Never install a filter from an untrusted source.

Save the dynamic-link library (DLL) associated with the add-in in a protected library (for example, %ProgramFiles%\Microsoft ISA Server). Be sure to configure strict ACLs for this library.

Disable application and Web filters that you do not require.

To disable an add-in, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Add-ins**:

- For ISA Server 2004 Enterprise Edition, for array-level add-ins, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, expand **Configuration**, and then click **Add-ins**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, expand **Configuration**, and then click **Add-ins**.

On the details pane, select the applicable add-in.

On the **Tasks** tab, click **Disable Selected Filters**.

System Policy

ISA Server includes a default system policy configuration, which allows use of services commonly required for the network infrastructure to function properly.

In general, from a security perspective, we strongly recommend that you configure the system policy so that access to services that are not required to manage your network is not allowed. After installation, carefully review the system policy rules configured. Similarly, after you perform major administration tasks, review the system policy configuration again.

The following sections describe services that are enabled by system policy rules.

Network Services

When you install ISA Server, basic network services are enabled. After installation, ISA Server can access name resolution servers and time synchronization services on the Internal network.

If the network services are available on a different network, you should modify the applicable configuration group sources to apply to the specific network. For example, suppose the DHCP server is not located on the Internal network, but on a perimeter network. Modify the source for the DHCP configuration group to apply to that perimeter network.

You can modify the system policy, so that only particular computers on the Internal network can be accessed. Alternatively, you can add additional networks, if the services are found elsewhere.

The following table shows the system policy rules that apply to network services.

Configuration group	Rule name	Rule description
DHCP	Allow DHCP requests from ISA Server to Internal Allow DHCP replies from DHCP servers to ISA Server	Allows the ISA Server computer to access the Internal network using Dynamic Host Configuration Protocol (DHCP) (reply) and DHCP (request).
DNS	Allow DNS from ISA Server to selected servers	Allows the ISA Server computer to access all networks using the Domain Name System (DNS) protocol.

Configuration group	Rule name	Rule description
NTP	Allow NTP from ISA Server to trusted NTP servers	Allows the ISA Server computer to access the Internal network using the NTP (UDP) protocol.

DHCP Services

If your DHCP server is not located on the Internal network, you must modify the system policy rule, so that it applies to the network on which the DHCP server is located. For example, if the DHCP server is located on the External network, perform the following procedure.

To modify the system policy rule, perform the following steps

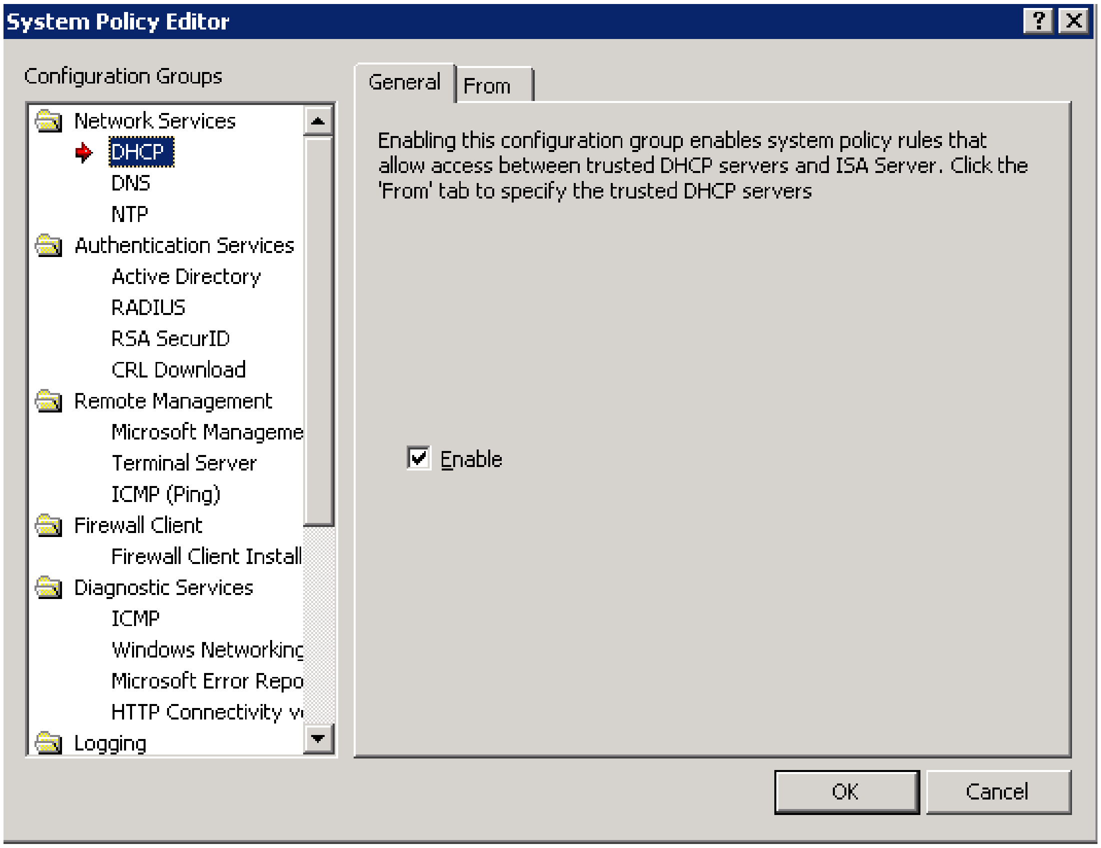
Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Firewall Policy**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Firewall Policy**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Firewall Policy**.

On the **Tasks** tab, click **Edit System Policy**.

In System Policy Editor, in the **Configuration Groups** tree, click **DHCP**.

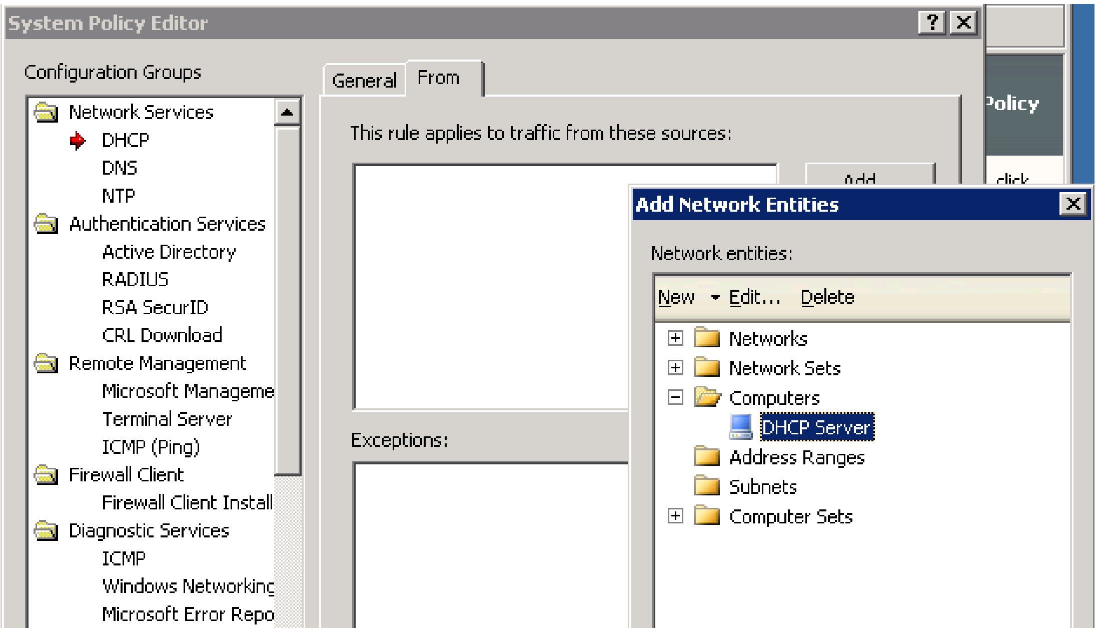


Enabling this configuration group enables system policy rules that allow access between trusted DHCP servers and ISA Server. Click the 'From' tab to specify the trusted DHCP servers

☑ Enable

On the **From** tab, click **Add**.

In **Add Network Entities**, select a network object.



Tip

We recommend that, if you know the IP address of the DHCP server, create a computer set with just that IP address and select that computer set. We strongly recommend this when the DHCP server is located on an untrusted network.

Click **Add**, and then click **Close**.

Authentication Services

One of the fundamental capabilities of ISA Server is the ability to apply a firewall policy to specific users. To authenticate users, however, ISA Server must be able to communicate with the authentication servers. For this reason, by default, ISA Server can communicate with Active Directory servers (for Windows authentication) and with RADIUS servers located on the Internal network.

The following table shows the system policy rules that apply to authentication services.

Configuration group	Rule name	Rule description
Active Directory	Allow access to directory services for authentication purposes Allow RPC from ISA Server to trusted servers Allow Microsoft CIFS from ISA Server to trusted servers Allow Kerberos authentication from ISA Server to trusted servers	Allows the ISA Server computer to access the Internal network using various Lightweight Directory Access Protocol (LDAP) protocols, remote procedure call (RPC) (all interfaces) protocol, various Microsoft common Internet file system (CIFS) protocols, and various Kerberos protocols, using Active Directory directory service.
RSA SecurID	Allow SecurID authentication from ISA Server to trusted servers	Allows the ISA Server computer to access the Internal network using the RSA SecurID® protocol.
RADIUS	Allow RADIUS authentication from ISA Server to trusted RADIUS servers	Allows the ISA Server computer to access the Internal network using various RADIUS protocols.
Certificate Revocation List	Allow HTTP from ISA Server to all networks for CRL downloads	Authentication Services: Allows Hypertext Transfer Protocol (HTTP) from ISA Server to selected networks for downloading updated certificate revocation lists (CRLs).

DCOM

If you require use of the DCOM protocol—for example, to remotely manage the ISA Server computer—be sure that you do not enable **Enforce strict RPC compliance**.

To verify that Enforce strict RPC compliance is not selected, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

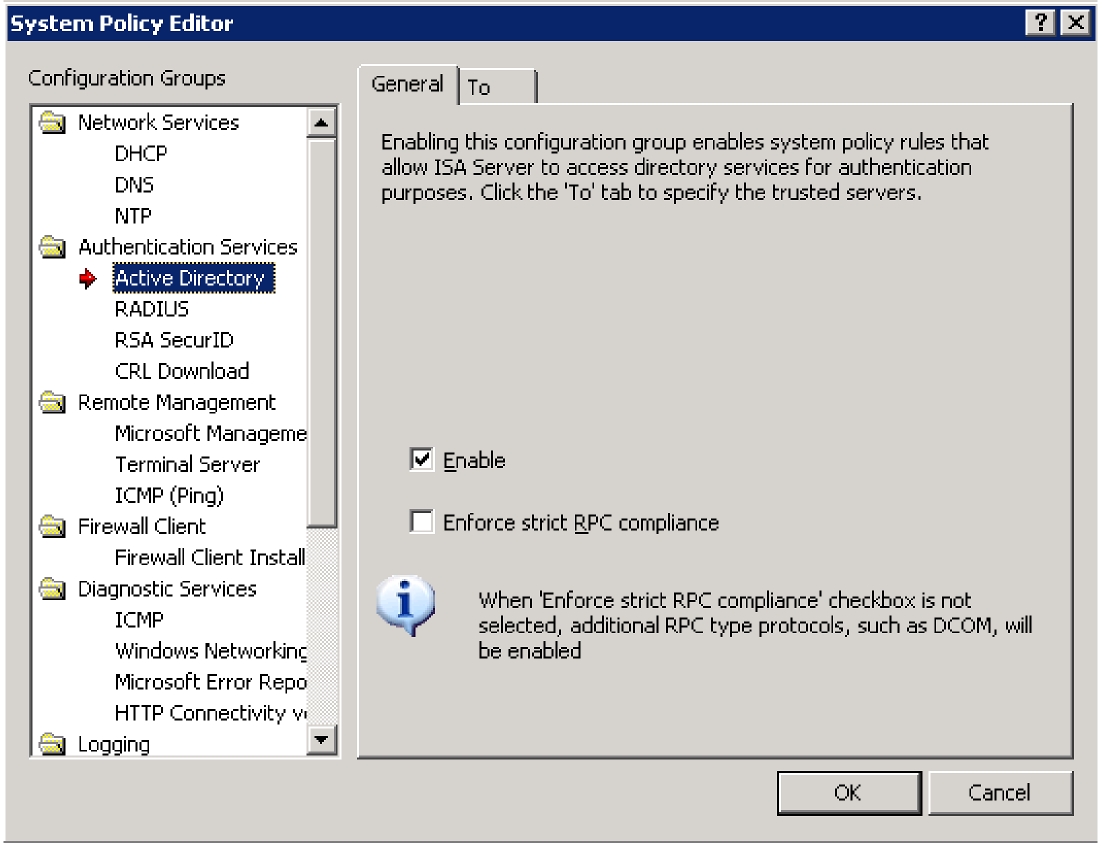
In the console tree of **ISA Server Management**, click **Firewall Policy**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Firewall Policy**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Firewall Policy**.

On the **Tasks** tab, click **Edit System Policy**.

In System Policy Editor, in the **Configuration Groups** tree, click **Active Directory**.

Verify that **Enforce strict RPC compliance** is not selected.



Enabling this configuration group enables system policy rules that allow ISA Server to access directory services for authentication purposes. Click the 'To' tab to specify the trusted servers.

☑ Enable

□ Enforce strict RPC compliance

When 'Enforce strict RPC compliance' checkbox is not selected, additional RPC type protocols, such as DCOM, will be enabled

Tip

DCOM is often required for various services, including remote management and auto-enrollment.

Windows and RADIUS Authentication Services

If you do not require Windows authentication or RADIUS authentication, you should perform the following steps to disable the applicable system policy configuration groups.

To disable the applicable system policy configuration groups, perform the following steps

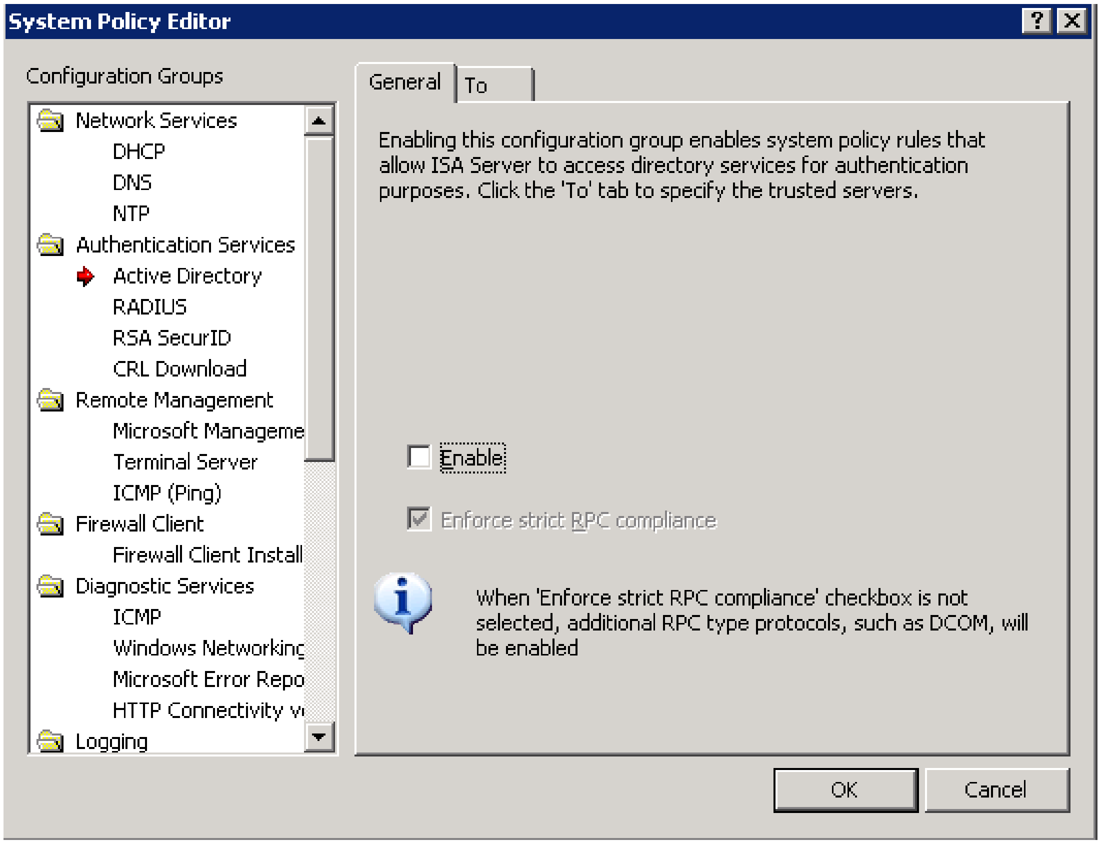
Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Firewall Policy**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Firewall Policy**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Firewall Policy**.

On the **Tasks** tab, click **Edit System Policy**.

In System Policy Editor, in the **Configuration Groups** tree, click **Active Directory**.



Enabling this configuration group enables system policy rules that allow ISA Server to access directory services for authentication purposes. Click the 'To' tab to specify the trusted servers.

□ Enable

☑ Enforce strict RPC compliance

When 'Enforce strict RPC compliance' checkbox is not selected, additional RPC type protocols, such as DCOM, will be enabled

On the **General** tab, verify that **Enable** is not selected.

Note

When you disable the Active Directory system policy configuration group, access to all LDAP protocols is effectively disabled. If you require the LDAP protocols, create an access rule allowing use of these protocols.

Repeat step 4 and step 5 for the RADIUS configuration group.

Tip

If you require only Windows authentication, be sure to configure the system policy, disabling use of all other authentication mechanisms.

RSA SecurID Authentication Services

Communication with RSA SecurID authentication servers is not enabled by default. If your firewall policy requires RSA SecurID authentication, be sure to enable this configuration group.

CRL Authentication Services

Certificate revocation lists (CRLs) cannot be downloaded by default. This is because the CRL Download configuration group is not enabled by default.

To enable CRL download, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Firewall Policy**:

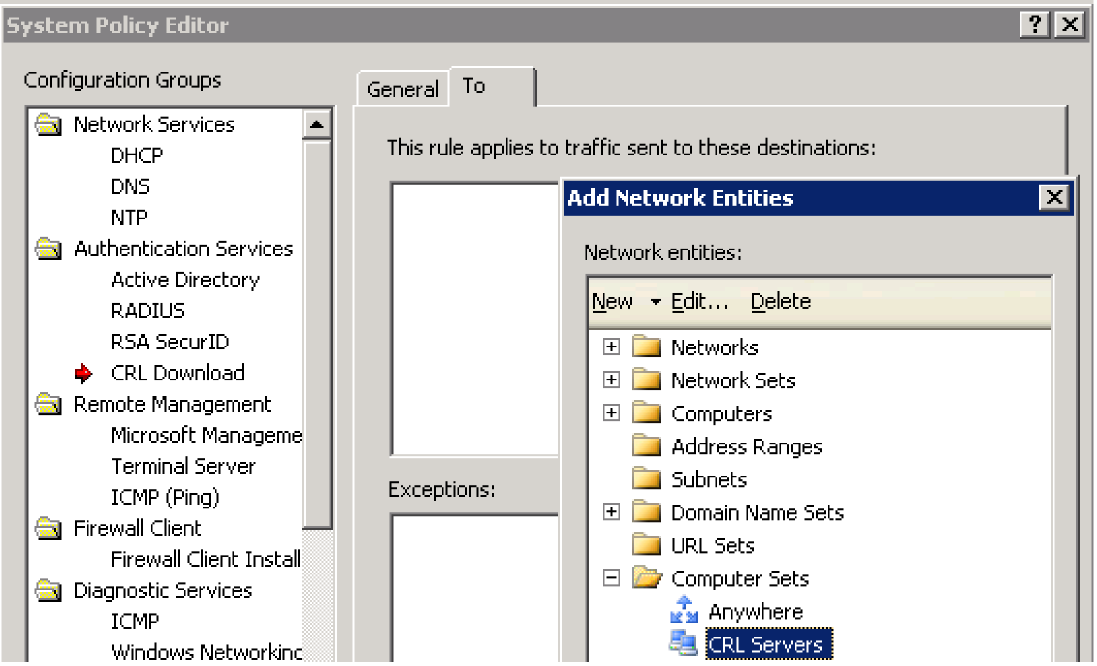
- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Firewall Policy**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Firewall Policy**.

On the **Tasks** tab, click **Edit System Policy**.

In System Policy Editor, in the **Configuration Groups** tree, click **CRL Download**.

On the **General** tab, verify that **Enable** is selected.

On the **To** tab, select the network entities from which certificate revocation lists can be downloaded.



This rule applies to traffic sent to these destinations:

All HTTP traffic will be allowed from the Local Host network (the ISA Server computer) to network entities listed on the **To** tab.

Remote Management

Often, you will manage ISA Server from a remote computer. Carefully determine which remote computers are allowed to manage and monitor ISA Server. The following table shows the system policy rules that should be configured.

Configuration group	Rule name	Rule description
Microsoft Management Console	Allow remote management from selected computers using MMC Allow MS Firewall Control communication to selected computers	Allows computers in the Remote Management Computers computer set to access the ISA Server computer using the MS Firewall Control and RPC (all interfaces) protocols.
Terminal server	Allow remote management from selected computers using Terminal Server	Allows computers in the Remote Management Computers computer set to access the ISA Server computer using the RDP (Terminal Services) protocol.
ICMP (Ping)	Allow ICMP (PING) requests from selected computers to ISA Server	Allows computers in the Remote Management Computers computer set to access the ISA Server computer using the PING protocol, and vice versa.

By default, the system policy rules allowing remote management of ISA Server are enabled. ISA Server can be managed by running a remote Microsoft Management Console (MMC) snap-in, or by using Terminal Services.

By default, these rules apply to the built-in Remote Management Computers computer set. When you install ISA Server, this empty computer set is created. Add to this empty computer set all computers that will remotely manage ISA Server. Until you do so, remote management is effectively not available from any computer.

Tip

Limit remote management to specific computers by configuring the system policy rules to apply only to specific IP addresses.

To enable remote management, perform the following steps

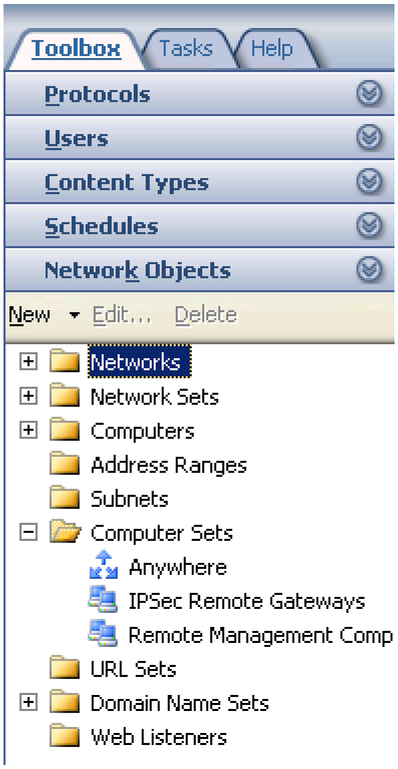
Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Firewall Policy**:

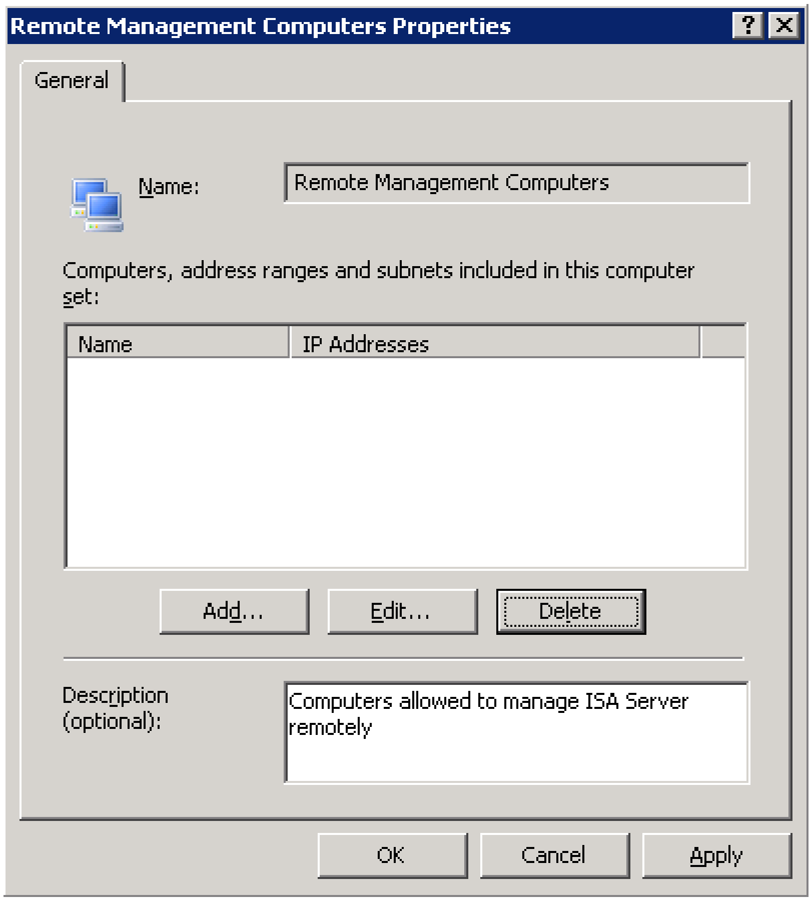
- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Firewall Policy**.

- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Firewall Policy**.

On the **Toolbox** tab, click **Network Objects**.



Expand **Computer Sets**, right-click **Remote Management Computers**, and then click **Properties**.


Remote Management Computers Properties
General
Name:
Computers, address ranges and subnets included in this computer set:
Name
IP Addresses
Add...
Edit...
Delete
Description (optional):
OK
Cancel
Apply

Name: Remote Management Computers

Description (optional): Computers allowed to manage ISA Server remotely

Click **Add**, and then click **Computer**.

In **Name**, type the name of the computer.

In **Computer IP Address**, type the IP address of the computer that can remotely manage ISA Server.

Remote Monitoring and Logging

By default, remote logging and monitoring is disabled. The following configuration groups are disabled by default:

Remote Logging (NetBIOS)

Remote Logging (SQL)

Remote Performance Monitoring

Microsoft Operations Manager

The following table provides a description of the configuration groups.

Configuration group	Rule name	Rule description
Remote logging (NetBIOS)	Allow remote logging to trusted servers using NetBIOS	Allows the ISA Server computer to access the Internal network using various NetBIOS protocols.
Remote Logging (SQL)	Allow remote SQL logging from ISA Server to selected servers	Allows the ISA Server computer to use Microsoft (SQL) protocols to access the Internal network.
Remote Performance Monitoring	Allow remote performance monitoring of ISA Server from trusted servers	Allows computers in the Remote Management Computers computer set to access the ISA Server computer using various NetBIOS protocols.
Microsoft Operations Manager	Allow remote monitoring from ISA Server to trusted servers, using Microsoft Operations Manager (MOM) Agent	Allows the ISA Server computer to access the Internal network using the Microsoft Operations Manager agent.

Enabling Remote Logging and Monitoring

Use the following procedure to enable remote logging and monitoring.

To enable remote monitoring and logging, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Firewall Policy**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Firewall Policy**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Firewall Policy**.

On the **Tasks** tab, click **Edit System Policy**.

In System Policy Editor, in the **Configuration Groups** tree, select one or more of the following configuration groups:

- Remote Logging (NetBIOS)
- Remote Logging (SQL)
- Remote Performance Monitoring
- Microsoft Operations Manager

On the **General** tab, verify that **Enable** is selected.

Firewall Client Share

If you installed the Firewall Client Share component when you installed ISA Server, the Firewall Client Installation Share configuration group is enabled, by default. All computers on the Internal network can access the shared folder. The following table shows the system policy configuration group (and rule) that is enabled.

Configuration group	Rule name	Rule description
Firewall client setup	Allow access from trusted computers to the Firewall Client installation share on ISA Server	Allows computers on the Internal network to access the ISA Server computer using various Microsoft CIFS and NetBIOS protocols. When you enable this rule, access is allowed to the ISA Server computer using SMB from any network or computer specified. Access is not limited only to the Firewall Client installation shared folder.

If you did not install the Firewall Client Share component, this configuration group is not enabled.

Diagnostic Services

By default, the system policy rules allowing access to diagnostics services are enabled, with the following permissions:

ICMP. This is allowed to all networks. This service is important for determining connectivity to other computers.

Windows networking. This allows NetBIOS communication, by default to computers on the Internal network.

Microsoft error reporting. This allows HTTP access to the Microsoft Error Reporting sites URL set, to allow reporting of error information. By default, this URL set includes specific Microsoft sites.

Connectivity verifiers. This allows the ISA Server computer to use HTTP and secure HTTP (HTTPS) protocols to check whether a specific computer is responsive.

The following table shows the system policy configuration groups that are enabled by default.

Configuration group	Rule name	Rule description
ICMP	Allow ICMP requests from ISA Server to selected servers	Allows the ISA Server computer to access all networks using various ICMP protocols and the PING protocol.
Windows networking	Allow NetBIOS from ISA Server to trusted servers	Allows the ISA Server computer to access all networks using various NetBIOS protocols.
Communication to Microsoft (Microsoft Error Reporting)	Allow HTTP/HTTPS from ISA Server to specified Microsoft error reporting sites	Allows the ISA Server computer to access members of the Microsoft Error Reporting sites URL set using HTTP or HTTPS protocols.

Connectivity Verifiers

In addition, the following diagnostic service is not enabled by default: HTTP Connectivity Verifiers.

When you create a connectivity verifier, the HTTP Connectivity Verifiers configuration group is enabled, allowing the Local Host network to use HTTP or HTTPS to access computers on any other network. The following table describes the HTTP Connectivity Verifiers configuration group.

Configuration group	Rule name	Rule description
HTTP Connectivity Verifiers	Allow HTTP/HTTPS from firewall to all networks, for HTTP connectivity verifiers	Allows the ISA Server computer to check for connectivity by sending HTTP GET requests to the specified computer.

We recommend that you limit this access to the specific computers whose connectivity you want to verify.

To limit this access, perform the following steps

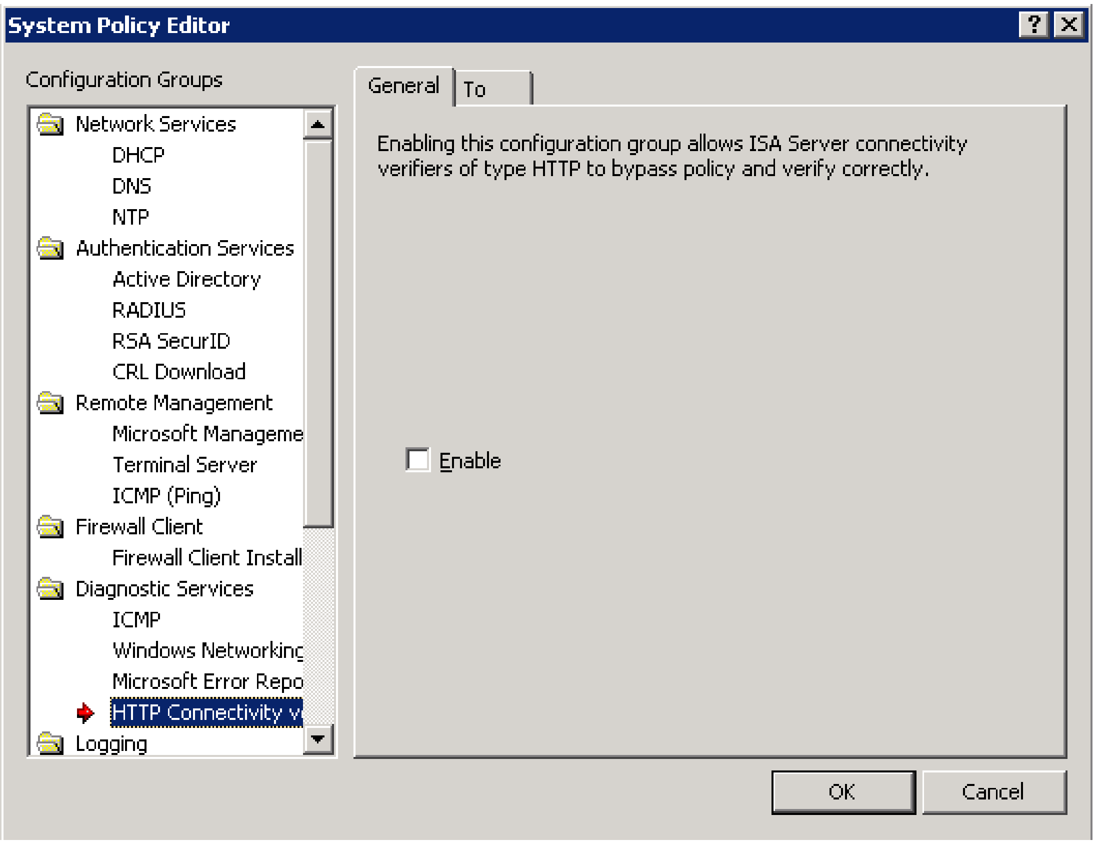
Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Firewall Policy**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Firewall Policy**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Firewall Policy**.

On the **Tasks** tab, click **Edit System Policy**.

In System Policy Editor, in the **Configuration Groups** tree, click **HTTP Connectivity verifiers**.



Enabling this configuration group allows ISA Server connectivity verifiers of type HTTP to bypass policy and verify correctly.

□ Enable

On the **To** tab, click **All Networks (and Local Host)** and then click **Remove**.

Click **Add** and then select the network entities whose connectivity you want to verify. All HTTP traffic will be allowed from the Local Host network (the ISA Server computer) to network entities listed on the **To** tab.

SMTP

By default, the Simple Mail Transfer Protocol (SMTP) configuration group is enabled, allowing SMTP communication from ISA Server to computers on the Internal network. This is required, for example, when you want to send alert information in an e-mail message. The following table describes the SMTP configuration group.

Configuration group	Rule name	Rule description
SMTP	Allow SMTP from ISA Server to trusted servers	Allows the ISA Server computer to access the Internal network using SMTP.

Scheduled Download Jobs

By default, the scheduled download jobs feature is disabled. The following table describes the Scheduled Download Jobs configuration group.

Configuration group	Rule name	Rule description
Scheduled Download Jobs	Allow HTTP from ISA Server to selected computers for Content Download Jobs	Allows the ISA Server computer to access all networks using HTTP.

When you create a content download job, you will be prompted to enable this system policy rule. ISA Server will be able to access the sites specified in the content download job.

Accessing the Microsoft Web Site

The default system policy allows HTTP and HTTPS access from the Local Host network (the ISA Server computer) to the Microsoft.com Web site. This is required for:

Error reporting (as described in the Diagnostic Services section).

Access to useful documentation on the ISA Server Web site and on other related Web sites.

By default, the Allowed Sites configuration group is enabled, allowing ISA Server to access content on specific sites that belong to the System Policy Allowed Sites domain name set. The following table describes the Allowed Sites configuration group.

Configuration group	Rule name	Rule description
Allowed Sites	Allow HTTP/HTTPS requests from ISA Server to specified sites	Allows the ISA Server computer to access members of the System Policy Allowed Sites URL set using HTTP and HTTPS protocols.

This URL set includes various Microsoft Web sites, by default. You can modify the domain name set to include additional Web sites, which ISA Server will be allowed to access.

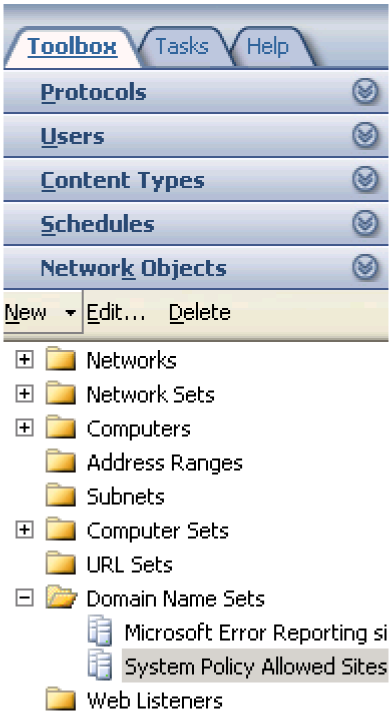
To modify the URL set to include additional Web sites, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Firewall Policy**:

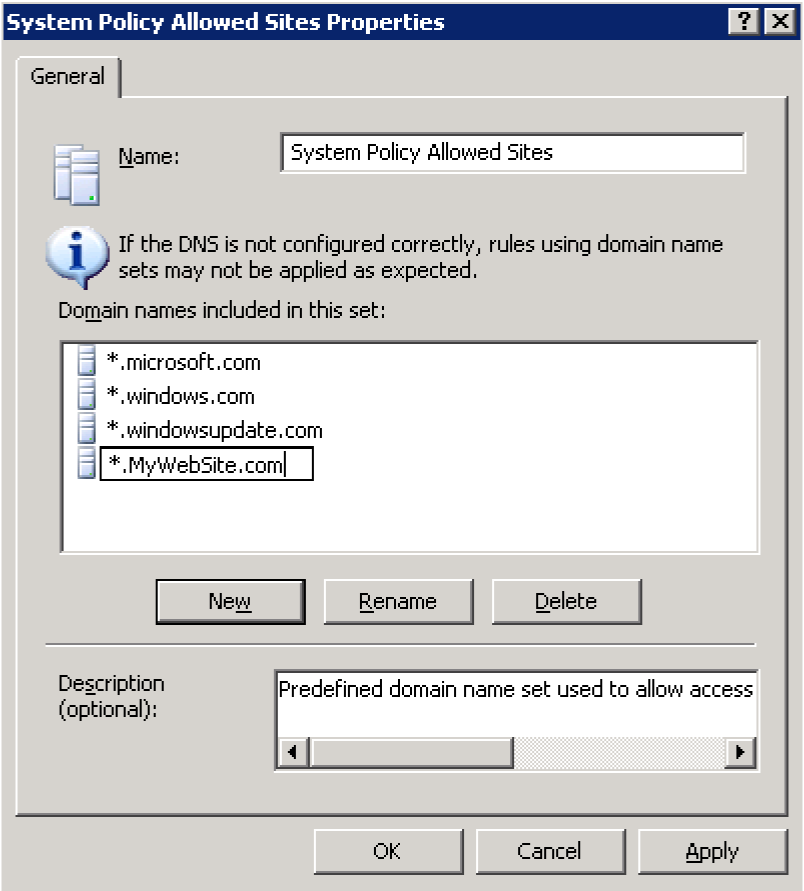
- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Firewall Policy**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Firewall Policy**.

On the **Toolbox** tab, click **Network Objects**.



Expand **Domain Name Sets**, right-click **System Policy Allowed Sites**, and then click **Properties**.

On the **General** tab, click **New**, and then type the URL for the specific Web site.



Name: System Policy Allowed Sites

If the DNS is not configured correctly, rules using domain name sets may not be applied as expected.

Domain names included in this set:

*.microsoft.com
*.windows.com
*.windowsupdate.com
*.MyWebSite.com

Description (optional): Predefined domain name set used to allow access

HTTP and HTTPS access will be allowed to the specified Web sites.

Lockdown Mode

A critical function of a firewall is to react to an attack. When an attack occurs, it may seem that the first line of defense is to disconnect from the Internet, isolating the compromised network from malicious outsiders. However, this is not the recommended approach. Although the attack must be handled, normal network connectivity must be resumed as quickly as possible, and the source of the attack must be identified.

The lockdown feature introduced with ISA Server 2004 combines the need for isolation with the need to stay connected. Whenever a situation occurs that causes the Microsoft Firewall service to shut down, ISA Server enters the lockdown mode. This occurs when:

An event triggers the Firewall service to shut down. When you configure alert definitions, you decide which events will cause the Firewall service to shut down. Essentially, you configure when ISA Server enters lockdown mode.

The Firewall service is manually shut down. If you become aware of malicious attacks, you can shut down the Firewall service, while configuring the ISA Server computer and the network to handle the attacks.

Affected Functionality

When in lockdown mode, the following functionality applies:

The Firewall Packet Filter Engine (fweng) applies the firewall policy.

Outgoing traffic from the Local Host network to all networks is allowed. If an outgoing connection is established, that connection can be used to respond to incoming traffic. For example, a DNS query can receive a DNS response, on the same connection.

No incoming traffic is allowed, unless a system policy rule that specifically allows the traffic is enabled. The one exception is DHCP traffic, which is always allowed. DHCP requests on UDP port 67 are allowed from the Local Host network to all networks, and DHCP replies on UDP port 68 are allowed back in.

The following system policy rules are still applicable:

- Allow ICMP from trusted servers to the local host.
- Allow remote management of the firewall using MMC (RPC through port 3847).
- Allow remote management of the firewall using RDP.

VPN remote access clients cannot access ISA Server. Similarly, access is denied to remote site networks in site-to-site VPN scenarios.

Any changes to the network configuration while in lockdown mode are applied only after the Firewall service restarts and ISA Server exits lockdown mode. For example, if you physically move a network segment and reconfigure ISA Server to match the physical changes, the new topology is in effect only after ISA Server exits lockdown mode.

ISA Server does not trigger any alerts.

Leaving Lockdown Mode

When the Firewall service restarts, ISA Server exits lockdown mode and continues functioning, as previously. Any changes made to the ISA Server configuration are applied after ISA Server exits lockdown mode.

Securing the Configuration

When you configure the ISA Server firewall policy in conjunction with your corporate security policy, follow the principle to deny all traffic that is not explicitly allowed. ISA Server by default implements this policy. A default firewall policy rule, named Default Rule, denies access by all users to all networks. Because this rule is processed last, any traffic not explicitly allowed will be denied.

Security Best Practices for Enterprise Management

ISA Server 2004 Enterprise Edition introduces a multi-tiered architecture, in which configuration information is stored on the Configuration Storage server. Array members communicate with the Configuration Storage server to get up-to-date configuration information. In addition, array members communicate with each other. To help secure this deployment model, follow the security best practices listed in this topic.

Securing the Configuration Storage Server

To secure the Configuration Storage server, follow these guidelines:

We recommend that you install the Configuration Storage server on a dedicated computer, which is not used for additional tasks.

Safeguard the security of the Configuration Storage server. Ensure that the computer is physically secure.

After you create administrator roles, avoid performing any tasks on the Configuration Storage server. Changes to the Configuration Storage server should be done using Enterprise Administrator credentials on an ISA Server array computer or remote management computer.

Users that belong to the Administrators group on the Configuration Storage server essentially have Enterprise Administrator permissions. This is because they can directly modify any data on the Configuration Storage server.

We recommend that you do not place the Configuration Storage server at the edge of the network. Rather, place it behind a computer running ISA Server services, which will help protect it from potential attacks.

Audit changes to permissions on the Configuration Storage server.

When possible, we recommend deploying a Configuration Storage server only in the corporate headquarters, and not in the branch offices. If a branch office has a good connection to headquarters, we recommend deploying a Configuration Storage server in headquarters to ensure a secured physical location for the Configuration Storage server. However, this is not recommended when the network connection to the branch office is slow.

Firewall Account Lockout

The Configuration Storage server recognizes each ISA Server array member by a unique account, especially created for this purpose. This account is not subject to account lockout. Potential denial-of-service attacks are prevented.

The default password on this account, created when you install the array member, is a strong password. If you change this password, we recommend that you configure a strong password.

Securing Intra-Array Communication

To secure intra-array communication, follow these guidelines:

Upon installation, a pair of private and public keys are created for each array member. These keys are used to transfer confidential data between array members. If you believe that the keys have been compromised, create a new key pair by uninstalling and then installing ISA Server.

We recommend that you use a dedicated network adapter in a network used only for intra-array communication. This network should include all the array member's intra-array addresses.

Validating Configuration After Upgrade

ISA Server 2000 policy can be migrated to ISA Server 2004, either by upgrading or by using the ISA Server Migration Wizard. Carefully review migrated policy. ISA Server 2004 employs a different rule model than ISA Server 2000. Make sure that the firewall policy is configured in accordance with your organization’s security policy.

Validating the Firewall Policy Configuration

After you create a firewall policy, we recommend that you actively check the policy. Validate that traffic that you want to pass through is being allowed. Also validate that only applicable ports are open.

For example, use port scanning to verify that only the applicable ports are actually open.

Local Domains

We recommend that you include all local domain names in the domains that are considered local to the Internal network. Otherwise, ISA Server may send a name resolution request to an external DNS server, thereby potentially exposing names of internal domains.

To configure the local domain table, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Networks**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, expand **Configuration**, and then click **Networks**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, expand **Configuration**, and then click **Networks**.

In the details pane, click the **Networks** tab, and then select the **Internal** network.

On the **Tasks** tab, click **Edit Selected Network**.

On the **Domains** tab, click **Add**. Then, type the domain name in **Enter a domain name to include**.

Backing Up and Restoring

ISA Server includes an export and import feature that enables you to back up and restore configuration information. The configuration parameters can be exported and stored locally in an .xml file. You can save your configuration to any directory and file name.

When you restore a configuration file, you potentially change the existing firewall policy. For this reason, take special care that you use only trusted configuration files when restoring (importing) the configuration information.

Virtual Private Networking

It is important to follow best practices for security when using ISA Server 2004 as a virtual private network (VPN) server. The following is a list of recommendations for securing your ISA Server computer in its role as a VPN server:

Layer Two Tunneling Protocol (L2TP) over Internet Protocol security (IPsec) connections are recommended for the strongest encryption. We recommend that you implement and enforce a strong password policy, thereby reducing the chance of a dictionary attack. When you implement such a policy, you can disable account lockout, thereby reducing the chance that an attacker will trigger account lockout.

Consider requiring your remote VPN clients to run particular operating systems (such as Microsoft Windows Server 2003, Windows 2000 Server, or Windows XP). Not all operating systems have equal levels of security in their file systems and in their user accounting. Also, not all remote access features are available on all operating systems.

Use the ISA Server Quarantine Control feature, to provide phased network access for remote VPN clients. With Quarantine Control, clients are restricted to a quarantine mode before allowed access to the network. Although Quarantine Control does not protect against attackers, computer configurations for authorized users can be verified and, if necessary, corrected before they can access the network.

Virus Protection with VPN

Virus infected VPN client computers are not automatically blocked from flooding the ISA Server computer or the networks it protects with requests. To prevent this occurrence, implement monitoring practices to detect anomalies such as alerts or unusual peaks in traffic loads, and configure alert notification to use e-mail messages. If an infected VPN client computer is identified, either:

Restrict VPN access by user name by using the remote access policy to exclude the user from the VPN clients who are allowed to connect.

Restrict VPN access by IP address. Do this by creating a new network to contain external IP addresses that are blocked, and move the IP address of the client out of the External network to the new network.

Authentication for VPN

Use authentication methods that provide adequate security. The most secure method of authentication is Extensible Authentication Protocol-Transport Level Security (EAP-TLS) when used in conjunction with smart cards. Despite the deployment challenges involved in using EAP-TLS and smart cards, which require a public key infrastructure (PKI), this is considered the most secure authentication method. Enable EAP-TLS, which is disabled by default on the profile of a remote access policy.

When you use the EAP-TLS authentication protocol, you must install a computer certificate on the Internet Authentication Service (IAS) server. For client and user authentication, you can install a certificate on the client computer, or you can use smart cards. Before you deploy certificates, you must design the certificate with the correct requirements.

If you use password-based authentication, enforce strong password policies on your network to make dictionary attacks more difficult.

Consider requiring your remote VPN clients to be authenticated with more secure authentication protocols, such as Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) or Extensible Authentication Protocol (EAP), rather than allowing them to use protocols such as Password Authentication Protocol (PAP), Shiva Password Authentication Protocol (SPAP), and Challenge Handshake Authentication Protocol (CHAP).

We strongly recommend that PAP, SPAP, and CHAP are disabled. PAP, SPAP, and CHAP are disabled by default.

IPsec Traffic

ISA Server does not block any encapsulating security payload (ESP) or authentication header (AH) traffic, which is part of IPsec traffic. Furthermore, such traffic is never considered spoofed, because these protocols are considered secure by design.

Network Load Balancing

For Enterprise Edition, for Network Load Balancing (NLB), follow these guidelines:

When you enable NLB, follow the security best practices detailed in *Network Load Balancing: Security Best Practices for Windows 2000 and Windows Server 2003* at the Microsoft TechNet Web site.

When you enable NLB, place a router in front of the NLB-enabled array. Configure the router so that it blocks raw IP traffic. Otherwise, all the array members will handle the traffic simultaneously.

When NLB is enabled, it synchronizes array members by using pure Ethernet protocol communication. This low-level traffic is not protected by ISA Server. To help secure that traffic, we strongly recommend that you place a Layer-3 router between the Internet and the NLB-enabled array. Also, place a Layer-3 router between the ISA Server computers and any network with untrusted computers.

This Layer-3 router will not allow the low-level Ethernet protocol to pass, thereby helping protect the array from potentially malicious Ethernet traffic from the Internet, intended to disrupt the operation of NLB.

Cache Array Routing Protocol

For Enterprise Edition, when you enable Cache Array Routing Protocol (CARP), follow these guidelines:

We recommend that you deploy a dedicated network for intra-array communication, and use this network for CARP communication. Otherwise, use a dedicated network for CARP communication. Configure Internet Protocol security (IPsec) for this network.

Networks for which CARP is enabled should be accessible only to array members.

Message Screener

When you create an SMTP Message Screener rule to hold a message, the Message Screener will store all messages that match the rule on the Message Screener computer in the %SYSTEMDRIVE%\inetpub\mailroot\badmail folder. The default ACL on this folder is READ ONLY for Authenticated Users (on computers running Windows Server 2003) and FULL CONTROL to everyone (on computers running Windows 2000 Server). We recommend that you configure the ACLs so that only authorized users can access the folder.

Link Translation

The link translation feature of ISA Server 2004 translates HTTP headers, regardless of whether link translation is enabled. This implies that when you publish a Web server, specifying that **Any domain name** can be used, an attacker could send malicious content in the header. If the published server redirects requests to a page on any computer, the response could be poisoned. (It would be modified to contain the URL from the header sent by the attacker.) If this page is cached by a downstream server, a user accessing the page would be redirected to the Web site configured by the attacker.

For this reason, we recommend that you specify specific domain names to which the Web publishing rule applies.

To specify specific domain names, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

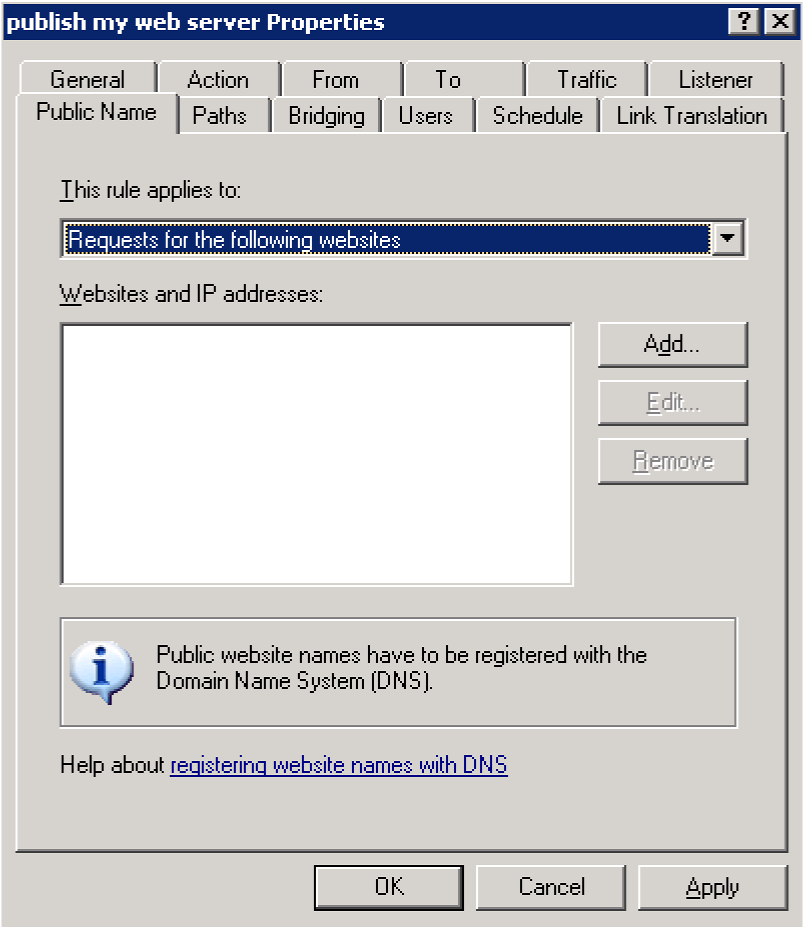
In the console tree of **ISA Server Management**, click **Firewall Policy**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Firewall Policy**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Firewall Policy**.

In the details pane, select the applicable Web publishing rule.

On the **Tasks** tab, click **Edit Selected Rule**.

On the **Public Name** tab, under **This rule applies to**, select **Requests for the following websites**.



This rule applies to: Requests for the following websites

Public website names have to be registered with the Domain Name System (DNS).

Help about registering website names with DNS

Click **Add**.

In **Public domain name or IP address**, type the specific domain name to which the Web publishing rule should apply.

Connection Limits

ISA Server limits the number of connections at any given time. You can configure the limit, specifying a maximum number of concurrent connections. When the maximum number of connections has been reached, any new client requests for that Web listener will be denied.

You can limit the total number of UDP, ICMP, and other Raw IP session creations allowed by a server publishing or access rule, per second. These limitations do not apply to TCP connections. When the specified number of connections is surpassed, new connections will not be created. Existing connections will not be disconnected.

We recommend that you configure low connection limits. You will effectively limit malicious hosts from consuming resources on the ISA Server computer.

By default, connection limits for non-TCP connections are configured to 1000 connections per second per rule, and to 160 connections per client. Connection limits for TCP connections are configured to 160 connections per client. We strongly recommend that you do not change these preconfigured limits. If you must modify the connection limits, configure as small a number of connections as possible.

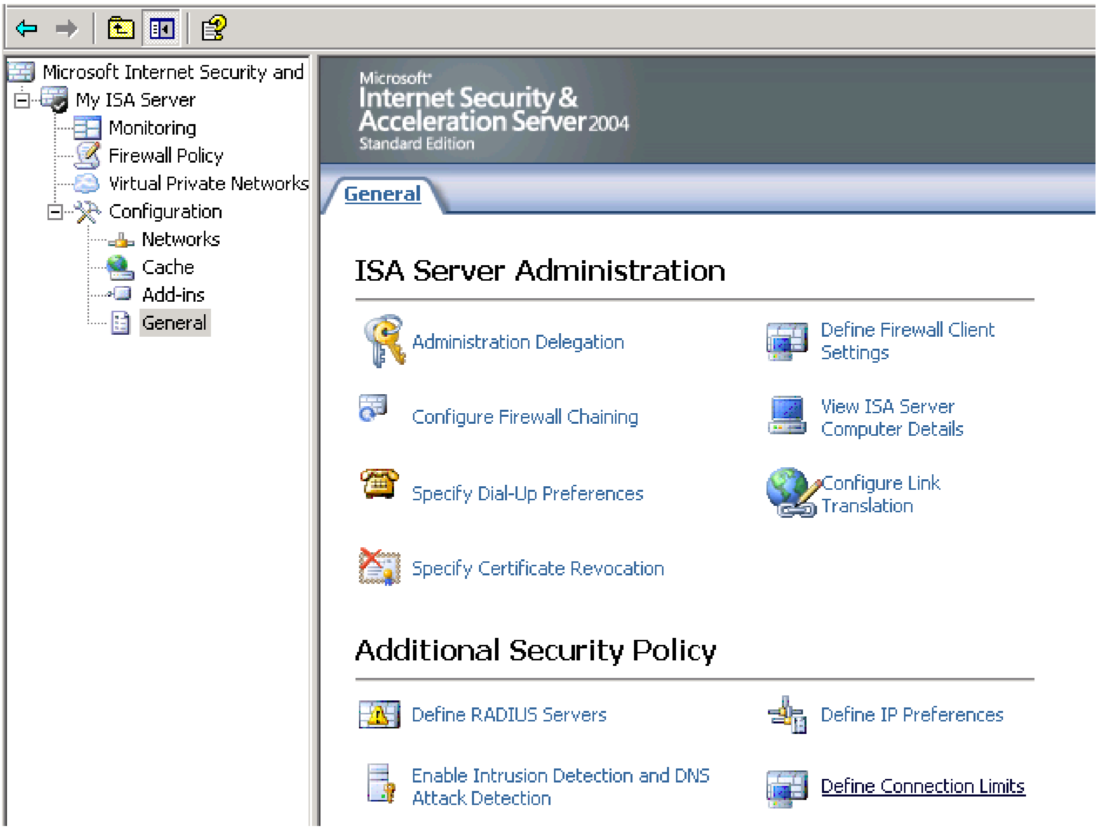
To configure connection limits, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

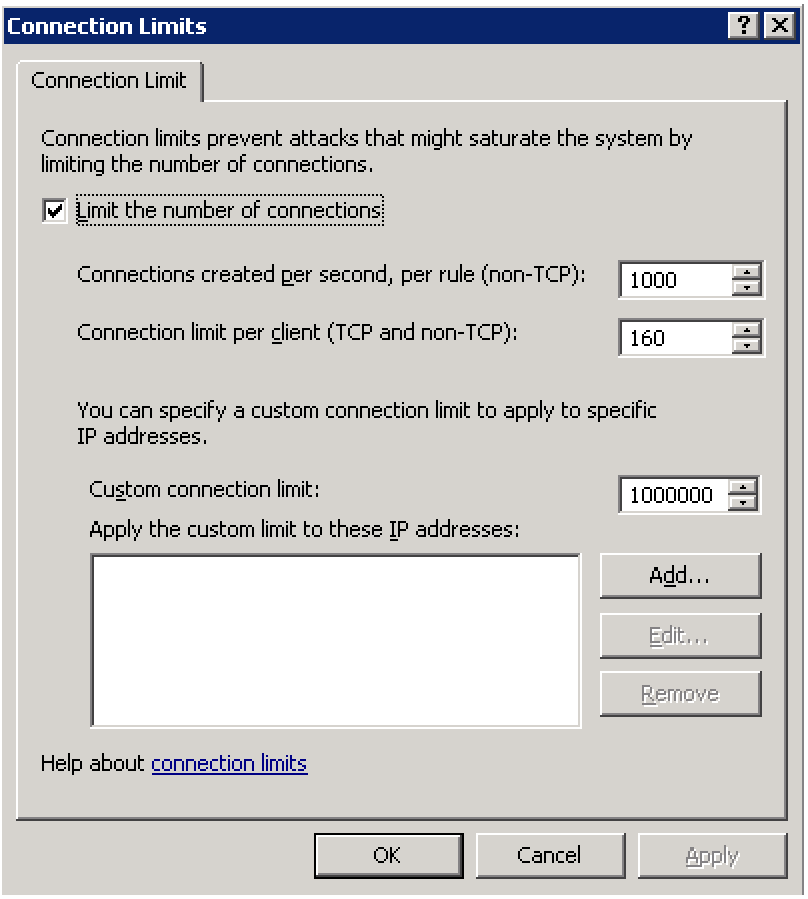
In the console tree of **ISA Server Management**, click **General**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, expand **Configuration**, and then click **General**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, expand **Configuration**, and then click **General**.

In the details pane, click **Define Connection Limits**.


Microsoft Internet Security and
My ISA Server
Monitoring
Firewall Policy
Virtual Private Networks
Configuration
Networks
Cache
Add-ins
General
Microsoft
Internet Security & Acceleration Server 2004
Standard Edition
General
ISA Server Administration
Administration Delegation
Define Firewall Client Settings
Configure Firewall Chaining
View ISA Server Computer Details
Specify Dial-Up Preferences
Configure Link Translation
Specify Certificate Revocation
Additional Security Policy
Define RADIUS Servers
Define IP Preferences
Enable Intrusion Detection and DNS Attack Detection
Define Connection Limits

On the **Connection Limit** tab, select **Limit the number of connections**.



Connection Limits

Connection Limit

Connection limits prevent attacks that might saturate the system by limiting the number of connections.

☑ Limit the number of connections

Connections created per second, per rule (non-TCP): 1000

Connection limit per client (TCP and non-TCP): 160

You can specify a custom connection limit to apply to specific IP addresses.

Custom connection limit: 1000000

Apply the custom limit to these IP addresses:

Help about connection limits

Do the following:

In **Connections created per second, per rule (non-TCP)**, type the number of connections allowed per rule, per second.

In **Connection limit per client (TCP and non-TCP)**, type the number of connections allowed per client.

Firewall Clients

ISA Server supports a more secure way of communication between the Firewall client and ISA Server, which involves the use of encryption using a TCP control channel. You can configure ISA Server to accept connections only from clients communicating in this secure way. However, this prevents earlier versions of Firewall Client software from connecting.

We recommend that you allow only Firewall clients that can communicate over an encrypted connection. This includes all the Firewall Client software for ISA Server 2004 computers.

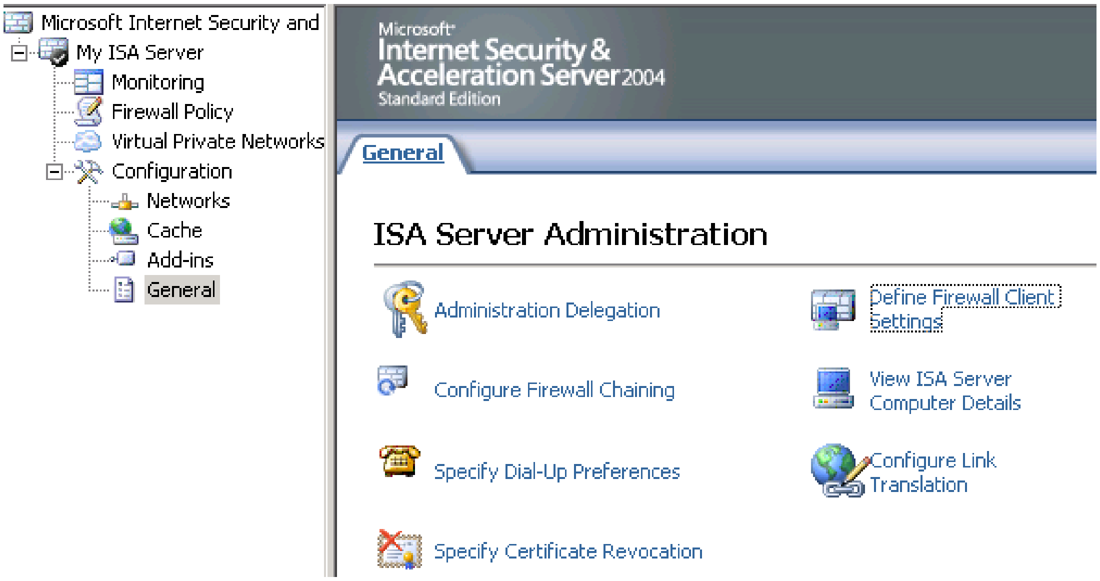
To configure Firewall clients, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

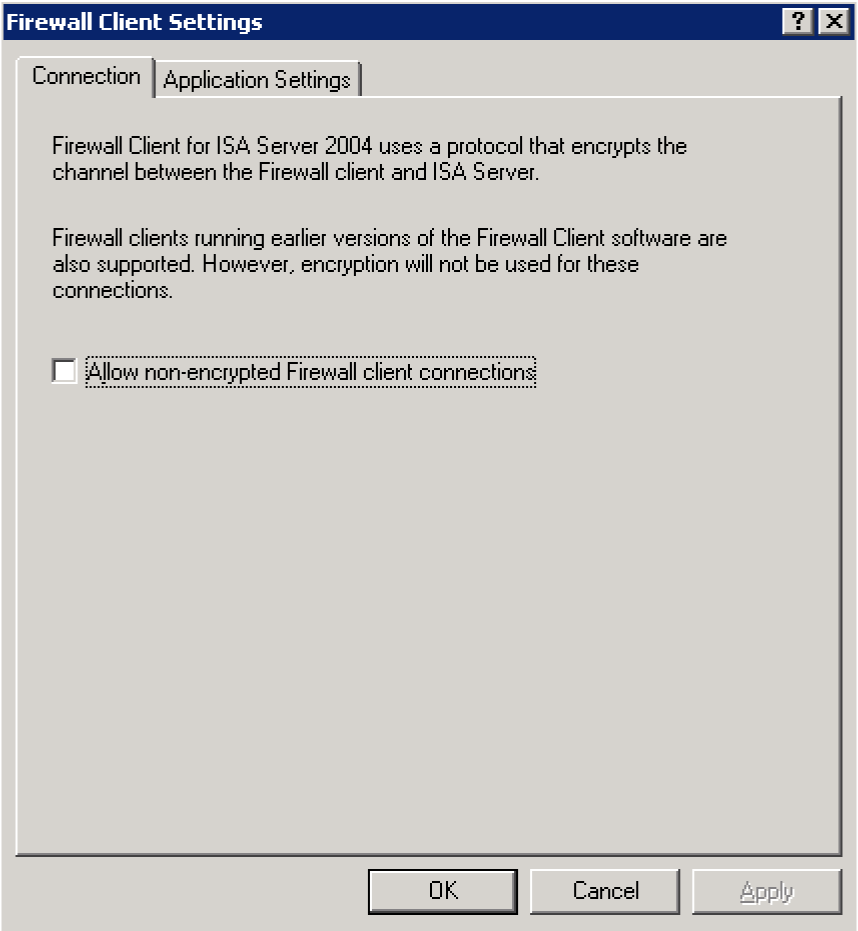
In the console tree of **ISA Server Management**, click **General**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, expand **Configuration**, and then click **General**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, expand **Configuration**, and then click **General**.

In the details pane, click **Define Firewall Client Settings**.


Microsoft Internet Security and
My ISA Server
Monitoring
Firewall Policy
Virtual Private Networks
Configuration
Networks
Cache
Add-ins
General
Microsoft Internet Security & Acceleration Server 2004
Standard Edition
General
ISA Server Administration
Administration Delegation
Define Firewall Client Settings
Configure Firewall Chaining
View ISA Server Computer Details
Specify Dial-Up Preferences
Configure Link Translation
Specify Certificate Revocation

On the **Connection** tab, verify that **Allow non-encrypted Firewall client connections** is not selected.



Firewall Client for ISA Server 2004 uses a protocol that encrypts the channel between the Firewall client and ISA Server.

Firewall clients running earlier versions of the Firewall Client software are also supported. However, encryption will not be used for these connections.

☐ Allow non-encrypted Firewall client connections

Firewall Chaining

When configuring firewall chaining, we recommend that you use IPsec to secure the communication channel between the ISA Server computer and the upstream server.

Securing the Deployment

The first step in securing ISA Server is verifying that the ISA Server computer is physically safe and that you apply basic security configuration recommendations.

After you secure the ISA Server computer and apply security guidelines when configuring the policy on the server, you should consider how to deploy the network infrastructure. This section describes security guidelines to consider when deploying a network secured by ISA Server.

Securing the Network Environment

To secure the network environment, perform the following:

Protect against Layer 2 attacks by deploying security solutions such as Layer 2 IDS and static MAC or port associations on switches.

Where possible, configure IPsec in the network.

To help protect from man-in-the-middle attacks on the Address Resolution Protocol (ARP) cache, we recommend that you place a router before the ISA Server computer. This is because ARP packets cannot be routed through a router. When ISA Server shares a physical network with an untrusted network, we recommend that you configure ISA Server to perform static ARP. For optimal security, we recommend that you add a static ARP entry for the default gateway and on other hosts on the same physical network.

Authentication

When configuring authentication for Web requests, use the strongest authentication method possible. We strongly recommend that you use the following authentication methods over connections that are not secure:

Basic

Digest

Outlook® Web Access forms-based authentication

SecurID

RADIUS

Using RADIUS Servers

Remote Authentication Dial-In User Service (RADIUS) is an industry standard protocol used to provide authentication. A RADIUS client (typically a dial-up server, VPN server, or wireless access point) sends user credentials and connection parameter information in the form of a RADIUS message to a RADIUS server. The RADIUS server authenticates the RADIUS client request, and sends back a RADIUS message response.

Because RADIUS servers authorize client credentials, in addition to authenticating them, the response that ISA Server receives from the RADIUS server, indicating that the client credentials are not approved, might actually indicate that the RADIUS server does not authorize the client. Even if the credentials have been authenticated, ISA Server may reject the client request, based on the RADIUS server authorization policy.

We recommend that you configure the RADIUS server as follows:

If you are using a RADIUS server for authentication, create a connectivity verifier that monitors the server status. Configure the alerts so that an appropriate action is taken when the RADIUS server is not functioning.

Untrusted users should not have access to the network between a RADIUS server and ISA Server. If untrusted users must have access, use IPsec on this network.

In addition, follow these guidelines when implementing a VPN or firewall policy that requires RADIUS authentication:

The RADIUS User-Password hiding mechanism might not provide sufficient security for passwords. The RADIUS hiding mechanism uses the RADIUS shared secret, the Request Authenticator, and the use of the MD5 hashing algorithm to encrypt the User-Password and other attributes, such as Tunnel-Password and MS-CHAP-MPPE-Keys. RFC 2865 notes the potential need for evaluating the threat environment and determining whether additional security should be used.

You can provide additional protection for hidden attributes by using Internet Protocol security (IPsec) with Encapsulating Security Payload (ESP) and an encryption algorithm, such as Triple DES (3DES), to provide data confidentiality for the entire RADIUS message. Follow these recommended guidelines:

- Use IPsec to provide additional security for RADIUS clients and servers.
- Require the use of strong user passwords.
- Use authentication counting and account lockout to help prevent a dictionary attack against a user password.
- Use a long shared secret with a random sequence of letters, numbers, and punctuation. Change it often to help protect your IAS server.

When you use password-based authentication, enforce strong password policies on your network to make dictionary attacks more difficult.

When user names are specified in any language other than English, ISA Server uses the current code page installed on the ISA Server computer to translate the user data. The user can be authenticated only if the client also uses the same code page.

If you change the RADIUS server policy while RADIUS-authenticated users are logged on, the new policy is not applied to users who are currently logged on. This is because ISA Server caches the credentials of users who are logged on, when users accessing the published Outlook Web Access server authenticate using RADIUS authentication. To apply the RADIUS server policy immediately, you can disconnect the session.

Client Authentication

When HTTP authentication is used to connect to the ISA Server firewall without Secure Sockets Layer (SSL), the request is potentially subject to a man-in-the-middle attack. The request could be altered by an attacker, during or after authentication.

To mitigate this attack, use HTTP authentication only with SSL-enabled connections.

Verifying Connectivity to Authentication Servers

If you are using a RADIUS server for authentication, create a connectivity verifier that monitors the server status. Configure the alerts so that an appropriate action is taken when the RADIUS server is not functioning.

To verify connectivity, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

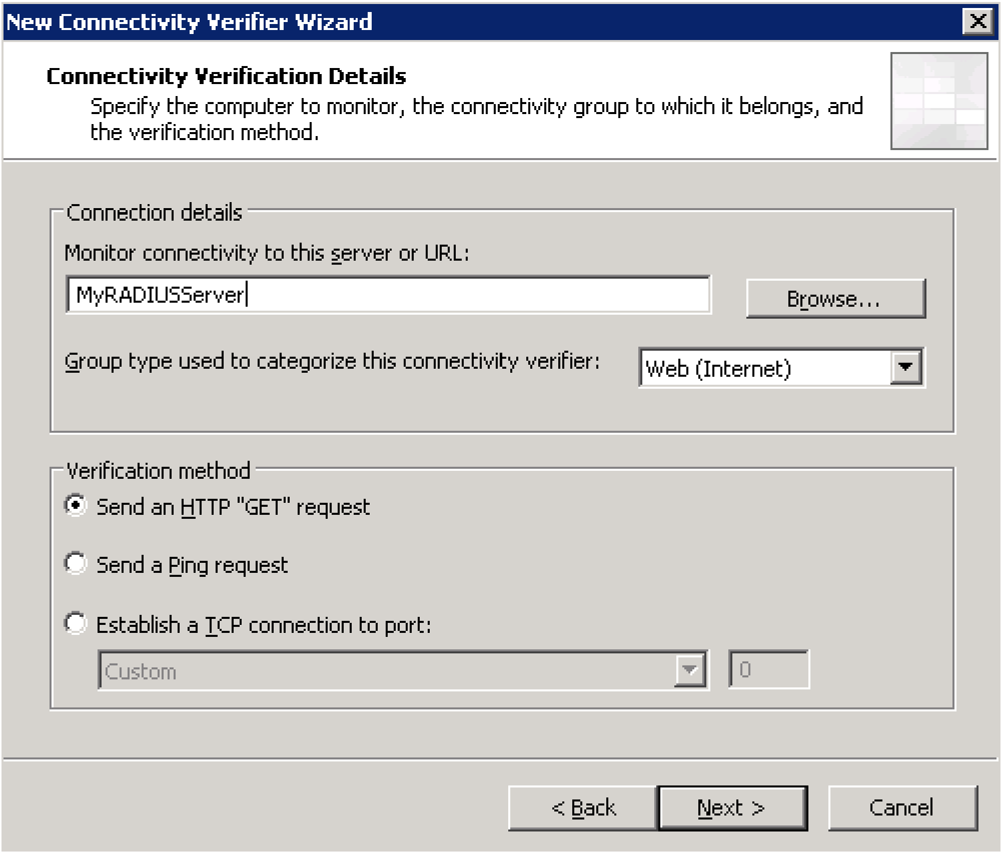
In the console tree of **ISA Server Management**, click **Monitoring**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Monitoring**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Monitoring**.

In the details pane, click the **Connectivity** tab.

On the **Tasks** tab, click **Create New Connectivity Verifier.**

On the **Welcome** page of the wizard, type a name for the connectivity verifier and then click **Next.**



New Connectivity Verifier Wizard

Connectivity Verification Details

Specify the computer to monitor, the connectivity group to which it belongs, and the verification method.

Connection details

Monitor connectivity to this server or URL: MyRADIUSServer

Group type used to categorize this connectivity verifier: Web (Internet)

Verification method

● Send an HTTP "GET" request

○ Send a Ping request

○ Establish a TCP connection to port:

Custom 0

On the **Connectivity Verification Details** page, do the following:

In **Monitor connectivity to this server or URL**, type the name of the server to monitor.

In **Verification method,** select a verification method. Click **Next** and then click **Finish**.

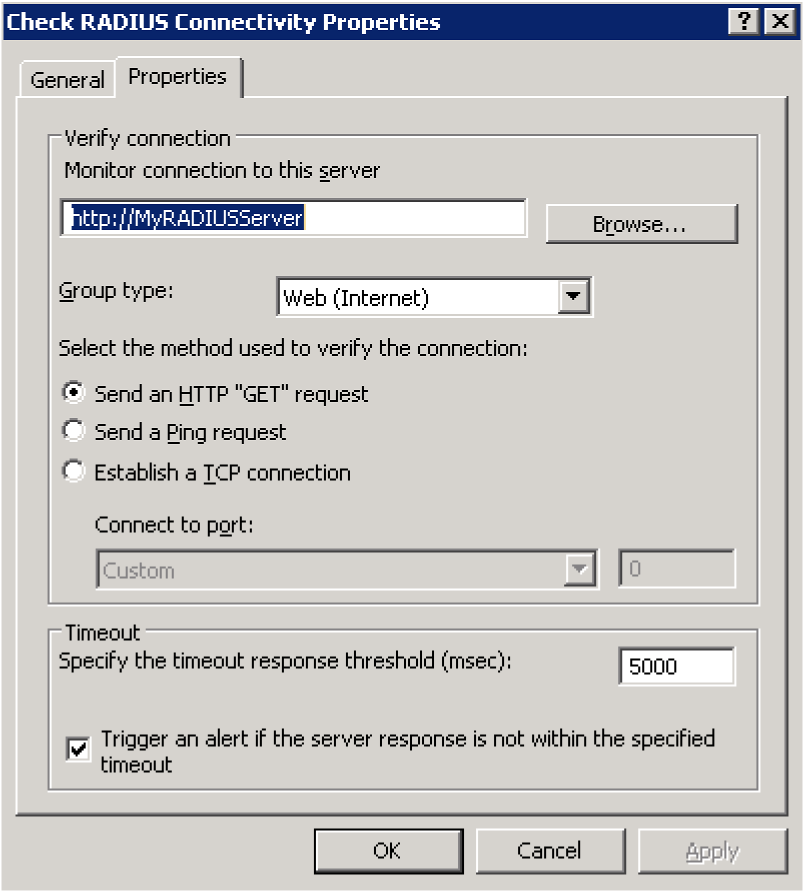
If the system policy rule that allows HTTP connectivity verification is not enabled, and you selected Send an HTTP "Get" request, you will be prompted to enable the system policy rule. Click Yes.

For more information about the HTTP connectivity verification system policy rules, see the Connectivity Verifiers section.

In the details pane, select the rule you just created.

On the **Tasks** tab, click **Edit Selected Verifier**.

On the **Properties** tab, verify that **Trigger an alert if the server response is not within the specified timeout** is selected.



Verify connection

Monitor connection to this server

http://MyRADIUSServer

Group type: Web (Internet)

Select the method used to verify the connection:

● Send an HTTP "GET" request

○ Send a Ping request

○ Establish a TCP connection

Connect to port:

Custom 0

Timeout

Specify the timeout response threshold (msec): 5000

☑ Trigger an alert if the server response is not within the specified timeout

Deploying Authentication Servers

For security reasons, we recommend that you place authentication servers in a highly secured network. Consider placing the authentication servers on a separate network (apart from the Internal and perimeter networks), when possible. You will effectively prevent direct access from any hosts on the Internal and perimeter networks to the authentication servers.

In this case, you should modify the applicable system policy rule, so that it applies to the network on which the authentication server is located.

To deploy authentication servers, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Firewall Policy**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Firewall Policy**.

- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Firewall Policy**.

On the **Tasks** tab, click **Edit System Policy**.

In System Policy Editor, in the **Configuration Groups** tree, under **Authentication Services**, click the applicable authentication method.

On the **To** tab, click **Add**.

In **Add Network Entities**, select the network on which the authentication server is located.

DNS Servers

Domain Name System (DNS) is the name resolution protocol for IP networks, such as the Internet. A DNS server hosts the information that enables client computers to resolve memorable, alphanumeric DNS names to the IP addresses that computers use to communicate with each other.

ISA Server includes a name resolution mechanism, similar to the DNS server name resolution mechanism. When a client makes a request to a host on another network, specifying the URL of the host computer, ISA Server can resolve the host computer name. ISA Server sends a name resolution request to the DNS server that you configure for its use.

To prevent DNS cache poisoning, we strongly recommend that you configure ISA Server to use a trusted DNS server (for example, a Windows DNS server), with the option to prevent cache pollution enabled. This DNS server should be located on the Internal network.

If you deploy a DNS server on an untrusted network (for example, on the External network), we recommend that you also install a DNS server on a trusted network (for example, a perimeter network). Then, configure the DNS server on the trusted network to forward requests to the DNS server on the untrusted network.

Follow these guidelines when deploying DNS servers:

Deploy a DNS server in the Internal network.

On the ISA Server computer, configure the network adapter connected to the Internal network to use the DNS server in the Internal network for all name resolution requests.

Verify that no other network adapter on the ISA Server computer uses an untrusted DNS server.

Create an access rule that allows only the internal DNS server to access the Internet for DNS resolution.

Important

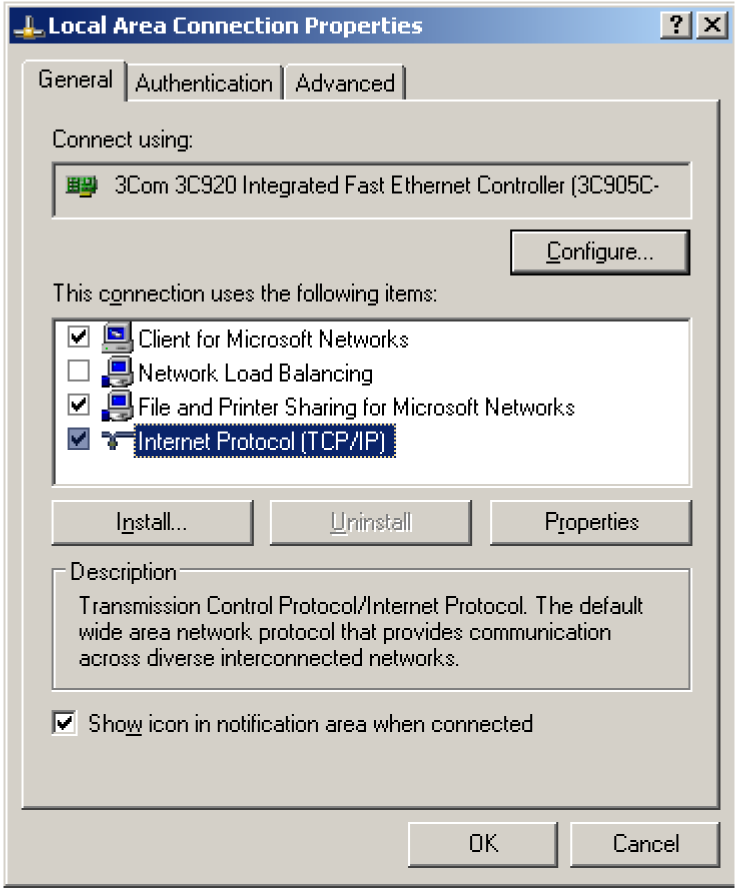
Only the trusted DNS server should send name resolution requests to the untrusted DNS server. No other server in the Internal network should directly access the untrusted DNS server.

To configure DNS, perform the following steps on the ISA Server computer

Click **Start**, point to **Control Panel**, and then double-click **Network Connections**.

Right-click the connection you want to configure, and then click **Properties**.

On the **General** tab, in **This connection uses the following items**, click **Internet Protocol (TCP/IP)**, and then click **Properties**.



Connect using:

3Com 3C920 Integrated Fast Ethernet Controller (3C905C-

This connection uses the following items:

☑ Client for Microsoft Networks
□ Network Load Balancing
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

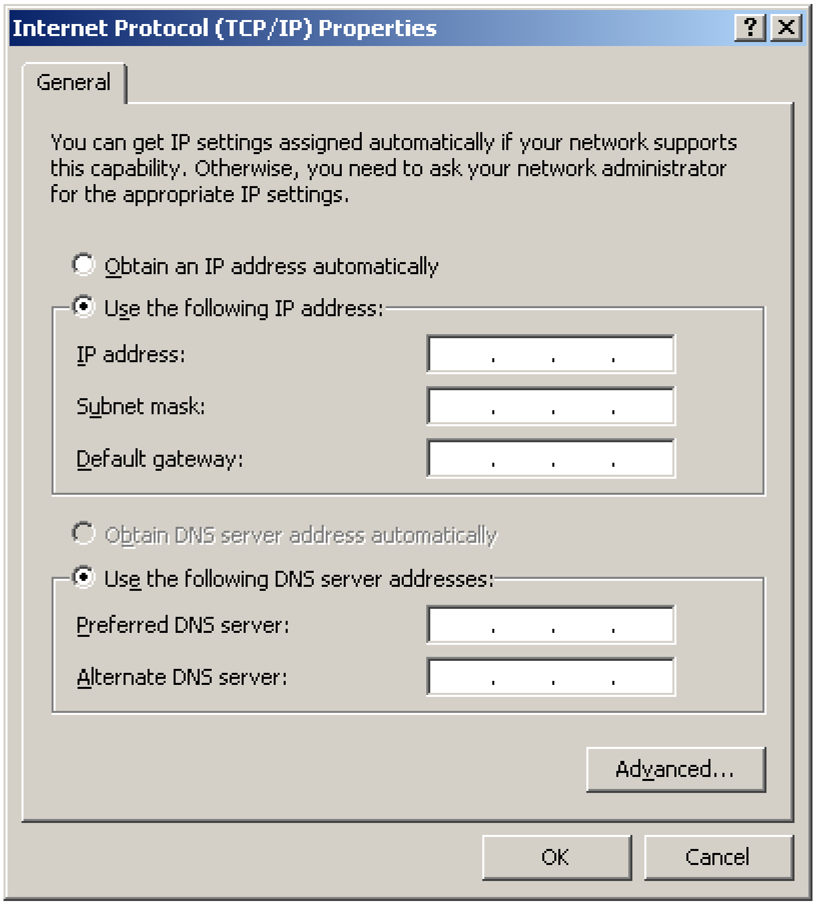
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

Select **Use the following DNS server addresses**.

In **Preferred DNS server** and in **Alternate DNS server**, type the IP addresses of a trusted DNS server on the Internal network.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Monitoring and Troubleshooting

An important and routine task that you will perform is monitoring the network traffic allowed to pass through ISA Server. A central part of the monitoring function is a careful analysis of the log and auditing information.

The following sections provide tips and hints about helping ensure log information integrity.

Logging

Logging gives you the opportunity to review network activity, checking who has been accessing resources on your network. Review the logs regularly and carefully, checking for suspicious access and usage of network resources. Follow these guidelines to make the best use of ISA Server logging:

Configure alerts to send notifications to administrators. Implement a rapid response procedure.

Save the logs to a separate NTFS disk partition for maximum security. Only administrators of the ISA Server computer should have access to the logs.

When you save log information to an SQL database, use Windows authentication (and not SQL authentication).

If you are logging the information to a remote database, configure encryption and data signature for the log information being copied to the remote database.

For maximal security, configure IPsec for the communication between the ISA Server computer and SQL Server.

If log information cannot be saved for any reason, lock down the ISA Server computer. To do so, configure an alert definition for the Log Failure event that stops the Firewall service.

Log Storage Limits

Use the log maintenance feature wisely, to ensure that the disk on which log information is stored does not become full.

Configure the Log Storage Limits alert definition to stop the ISA Server services. You only allow access when the access can be appropriately audited.

To configure log storage limits, perform the following steps

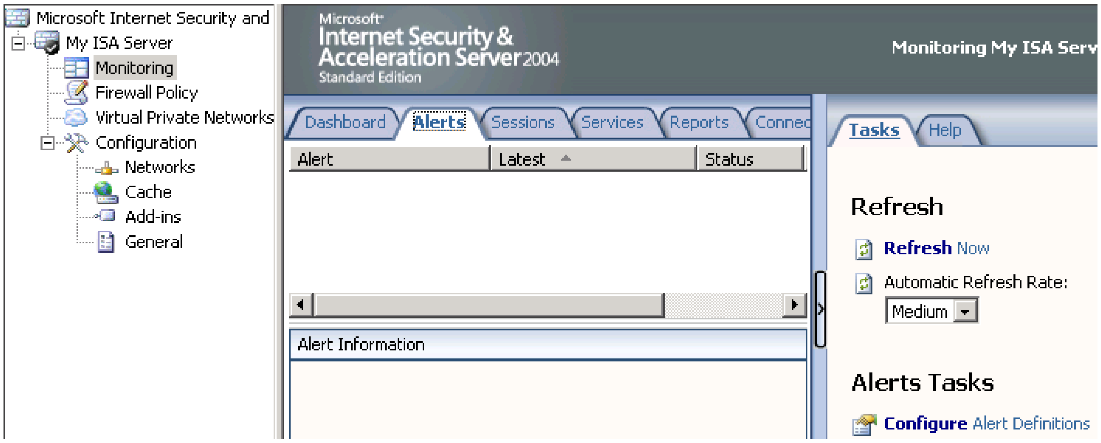
Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Monitoring**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, and then click **Monitoring**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, and then click **Monitoring**.

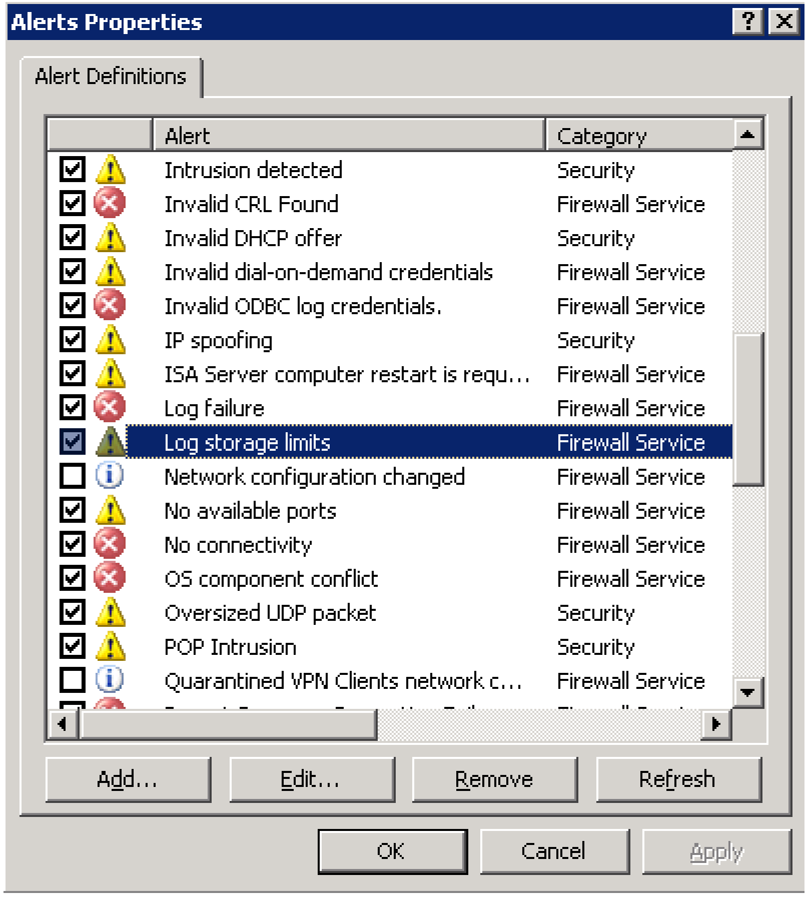
In the details pane, click the **Alerts** tab.

On the **Tasks** tab, click **Configure Alert Definitions**.



Automatic Refresh Rate: Medium

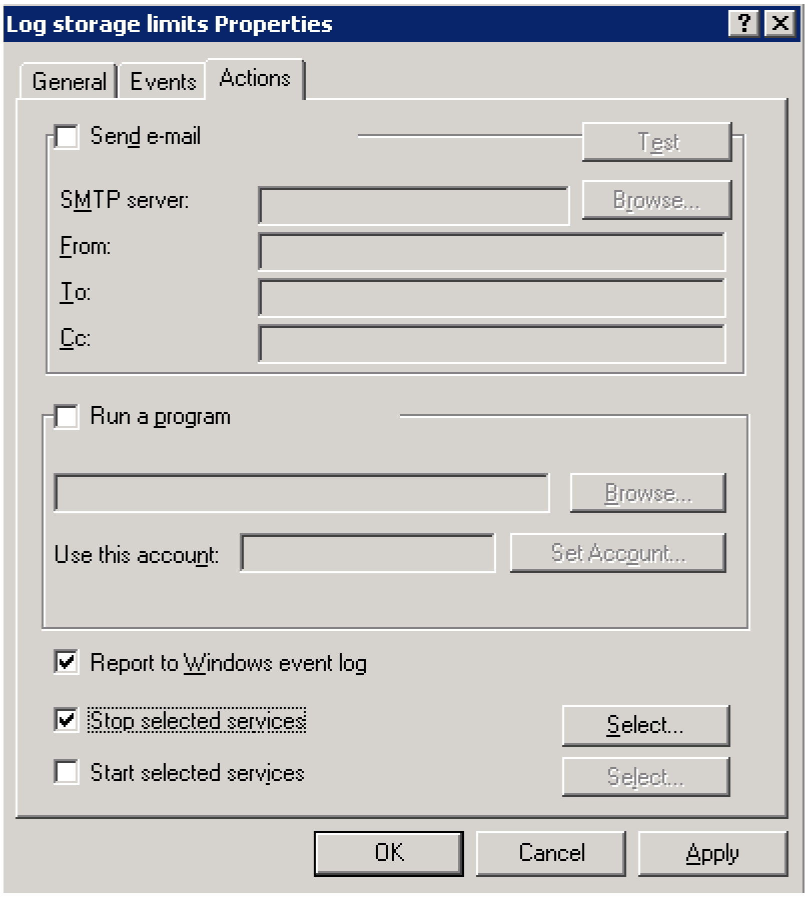
In **Alert Definitions**, click **Log storage limits**, and then click **Edit**.



		Alert	Category
☑	⚠	Intrusion detected	Security
☑	⊗	Invalid CRL Found	Firewall Service
☑	⚠	Invalid DHCP offer	Security
☑	⚠	Invalid dial-on-demand credentials	Firewall Service
☑	⊗	Invalid ODBC log credentials.	Firewall Service
☑	⚠	IP spoofing	Security
☑	⚠	ISA Server computer restart is requ...	Firewall Service
☑	⊗	Log failure	Firewall Service
☑	⚠	Log storage limits	Firewall Service
☐	ⓘ	Network configuration changed	Firewall Service
☑	⚠	No available ports	Firewall Service
☑	⊗	No connectivity	Firewall Service
☑	⊗	OS component conflict	Firewall Service
☑	⚠	Oversized UDP packet	Security
☑	⚠	POP Intrusion	Security
☐	ⓘ	Quarantined VPN Clients network c...	Firewall Service

On the **General** tab, select **Enable**.

On the **Actions** tab, click **Stop selected services**, and then click **Select**.



□ Send e-mail

SMTP server:

From:

To:

Cc:

□ Run a program

Use this account:

☑ Report to Windows event log

☑ Stop selected services

□ Start selected services

In **Services**, select **Microsoft Firewall** and **Microsoft ISA Server Job Scheduler**.

Auditing

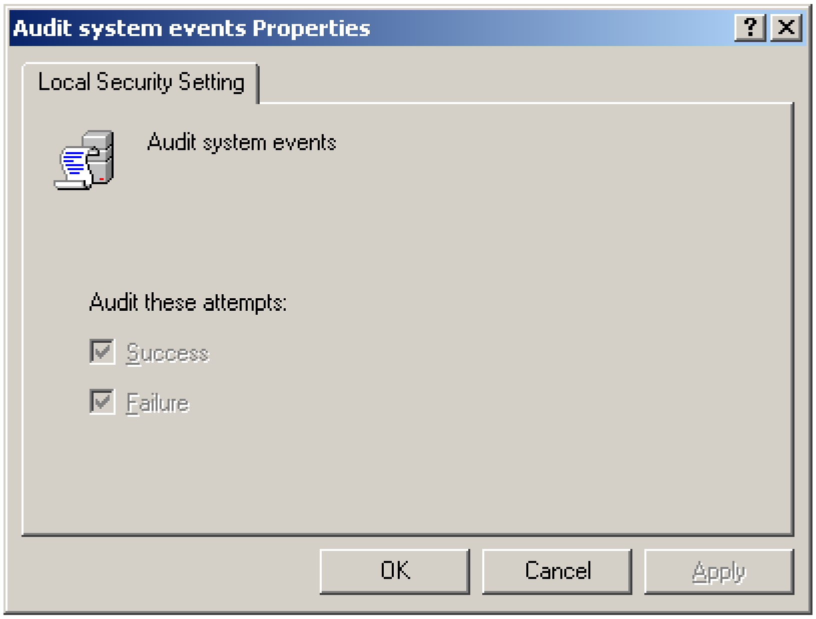
Enable Windows auditing, so that you can monitor who logs on to the ISA Server computer.

To enable auditing, perform the following steps on the ISA Server computer

Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Local Security Policy**.

Expand **Security Settings**, expand **Local Policies**, and then click **Audit Policy**.

In the details pane, right-click **Audit logon events**, and then click **Properties**.



Audit system events

Audit these attempts:

☑ Success

☑ Failure

Select **Success** and **Failure**.

Floods

A flood attack occurs when an attempt is made to deny services to legitimate users by intentionally overloading a network. Flood attacks might occur, for example, when a worm tries to propagate outside of your corporate network.

The first symptoms that show that ISA Server is experiencing a flood attack are a sudden surge in CPU utilization, increased memory consumption, or very high logging rates on the ISA Server computer.

If you determine that the ISA Server computer is experiencing a flood attack, use the log viewer, to determine the source of the offending traffic. Specifically, look for the following:

Log entries for denied traffic. Pay special attention to traffic that is denied because the quota is exceeded, spoofed packets, and packets with corrupted CHECKSUM. These usually are indicative of a malicious client. In ISA Server 2004 Standard Edition, connections that are terminated due to exceeding the connections limit will have a result code of 0x80074e23. In ISA Server 2004 Enterprise Edition, the result will appear as text, which clearly indicates the connection termination reason.

Logs that indicate numerous connections that are created and then immediately closed. This often indicates that a client computer is scanning an IP address range for a specific vulnerability.

Another way to detect and list the offending computers is to temporarily reconfigure the Connection Limit alerts to be triggered every one second (instead of **Manually Reset**). A list of alerts is generated, each one indicating the offending IP address in the alert text. After you identify the list of offending IP addresses, perform the following procedure to improve the performance of ISA Server during the flood.

To improve ISA Server performance during a flood, perform the following steps

Disable logging. Disable logging either on the specific rule that matches the flood or altogether until the flood attack is stopped.

Reconfigure the Connections Limit alerts (or any other types of alerts that may be triggered repeatedly as a result of the specific attack) back to **Manually Reset**.

Connection Limit Alert

When a Connection Limit alert occurs, determine whether your network is being attacked, or whether there is simply a heavy load of valid traffic. If the limit was exceeded due to malicious traffic, try the following:

If the malicious traffic appears to originate from the Internal network, this may indicate a virus on the Internal network. Identify the source IP address, and disconnect the computer from the network immediately.

If the malicious traffic appears to originate from a small range of IP addresses on an External network, create a rule denying access to a computer set that includes the source IP addresses.

If the traffic appears to originate from a large range of IP addresses, evaluate the overall status of your network. Consider setting a smaller connection limit, so that ISA Server can better protect your network.

In addition, we recommend that you limit the number of connections, because this can help prevent flood attacks. When a UDP or raw IP flood attack occurs, many requests are sent from spoofed source IP addresses, eventually resulting in a denial of service.

Protecting from Floods Caused by Worms and Viruses

Your Internal network could be exposed to infection by the following types of worms:

Worms that infiltrate using a specific protocol.

Worms that are destined for specific IP addresses.

Worms that originate from specific IP addresses.

To help protect your Internal network from worms and other malicious software, we recommend the following:

Enable quarantine protection on the VPN Clients network.

Create an access rule that denies traffic to and from infected clients, and denies use of the protocols used by the worms. Do not enable logging for this rule.

Configure a disconnected network that includes IP addresses of infected clients. Any traffic originating from these clients will be dropped as spoofed.

Creating a Disconnected Network

A disconnected network represents a range of IP addresses that are not physically connected to the ISA Server computer.

To create a disconnected network, perform the following steps

Click **Start**, point to **All Programs**, point to **Microsoft ISA Server**, and then click **ISA Server Management**.

In the console tree of **ISA Server Management**, click **Networks**:

- For ISA Server 2004 Enterprise Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand **Arrays**, expand ***Array_Name***, expand **Configuration**, and then click **Networks**.
- For ISA Server 2004 Standard Edition, expand **Microsoft Internet Security and Acceleration Server 2004**, expand ***Server_Name***, expand **Configuration**, and then click **Networks**.

In the details pane, click the **Networks** tab.

On the **Tasks** tab, click **Create a New Network.**

On the **Welcome** page, type the name of the network. For example, type **Disconnected**, and then click **Next**.

On the **Network Type** page, select **External Network**, and then click **Next**.

On the **Network Addresses** page, click **Add**. Then, in **Starting address** and in **Ending address**, type the IP addresses of the infected clients. Click **OK**, click **Next**, and then click **Finish**.

In the details pane, click the **Network Rules** tab. Check that there are no network rules that apply to this network.

Note

Be sure to update this network each time another client is identified as infected.

Configuring the Routing Table

By adjusting the local routing table on the ISA Server computer, you can help ensure that infected clients are not allowed access to resources on your Internal network. Do the following:

Add another network adapter to the ISA Server computer. Do not associate it with any ISA Server network.

Use the **route add** command to add static routes to the IP addresses of the infected clients using the IP address of this network adapter.

Hostile Code

If a user unknowingly executes hostile code, and that hostile code has been packaged with additional files including modified versions of system DLLs, the hostile code could load its own versions of those DLLs, potentially increasing the type and degree of damage the code can render. Configure the registry key MSS: Enable Safe DLL search mode (recommended) to a value of Enabled.

For more information about this registry key, see "Chapter 10: Additional Registry Settings" in the *Threats and Countermeasures Guide* at the Microsoft TechNet Web site.

Additional Resources

Additional ISA Server 2004 documents are available at the ISA Server 2004 Guidance page.

Do you have comments about this document? Send feedback.