Net Report Configuration Guide for Microsoft ISA Server

Table of Contents

Section 1: About This Document

This document explains how to configure Microsoft ISA Server for NetReport.

1.1. Scope

This document coves the following topics:

- Installing Microsoft ISA Server,
- Configuring Microsoft ISA Server,
- Log Value Reference Section
- ISA Default Settings Reference Section
- Further Reading

1.2. Audience

This document addresses both basic and advanced Net Report users.

1.3. Related Information

Please read the following documents which are related to Net Report's technical documentation:

Copyright Notice:

http://www.net-report.net/downloads/WebDoc/Copyright/Net_Report_Copyright_Notice.pdf

Code and Icon Conventions:

http://www.net-report.net/downloads/WebDoc/Conventions/Net_Report_Code_and_Icon_Conventions.pdf

Online Help:

http://www.net-report.net/us/support/sup_userhelp.html

Troubleshooting:

http://www.net-report.net/us/OurDocuments/NRFAQs.htm

Glossary:

http://www.net-report.net/knowledgebase/UserHelp/16_Net_Report_Glossary/Net_Report_Glossary_2.0.1.htm

Section 2: Installing Microsoft ISA Server Software

2.1. Installation Procedure

Follow these steps to install ISA Server software:

Steps

1. Insert the **ISA Server CD** into the CD drive, or run `ISAautorun.exe` from the shared network drive.

2. Click **Install ISA Server** in Microsoft ISA Server Setup.

3. Click **Next** after the setup program prompts that it has completed determining the system configuration.

4. Click **I accept the terms in the license agreement**, if you accept the terms and conditions stated in the end-user license agreement.

5. Click **Next**.

6. Type your customer details.

7. Click **Next**.

2.2. Choosing the Installation Type

Steps

1. Click **Typical Installation**, **Full Installation**, or **Custom Installation**.

2. If you click **Custom Installation**, select the check boxes which correspond to the ISA Server components you want to install. Select from the following:

- **ISA Server Services**
- **ISA Server Management**
- **Firewall Client Installation Share**
- **Message Screener**

3. Click **Next**.

2.3. Configuring the Internal Network

To configure the Internal network. Follow the following steps:

Steps

1. Click **Add**.

2. Click **Configure Internal Network**.

3. Select **Add address ranges based on the Windows Routing Table**.

4. Select one or more of the adapters, which are connected to the Internal network. These addresses will be included in the Internal network that is defined by default for ISA Server.

5. Clear the selection of **Add the following private IP ranges**, unless you want to add those ranges to your Internal network.

6. Click **OK**.

7. Click **OK** again to finish the Internal network configuration.

8. Click **Next**.

9. Click **Install**.

Note: if you want to invoke ISA Server Management immediately, select the **Invoke ISA Management** check box, and then click **Finish**.

Section 3: Configuring Microsoft ISA Server for Net Report

Overview

This section details how to configure Microsoft ISA Server for Net Report Log Analyser.

3.1. Configuring ISA Management

Steps

Either

1. Select **Start> Programs> Microsoft ISA Server> ISA Management** to open Microsoft ISA Management.

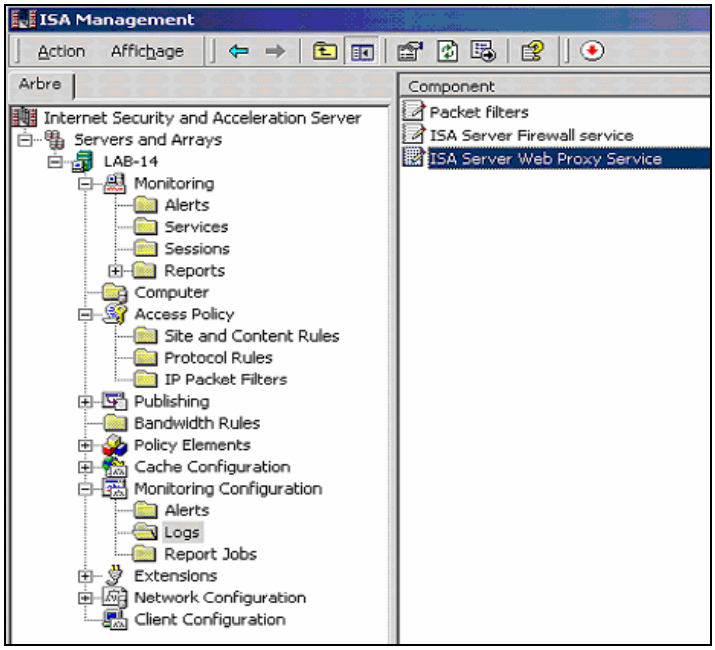
Or

2. Select `ISA Management.Ink`.

ISA Management.lnk

Then

3. Configure logging to a file, in the console tree of **ISA Management**, by selecting the **Internet Security and Acceleration Server** icon in the tree structure. The sub-items will appear.



4. Click the plus icon next to **Servers and Arrays**.

5. Select your Server Name.

6. Click the plus icon next to **Monitoring Configuration** to display the subitems.

7. Select the **Logs** directory.

3.2. Configuring Logging Options

To configure logging options:

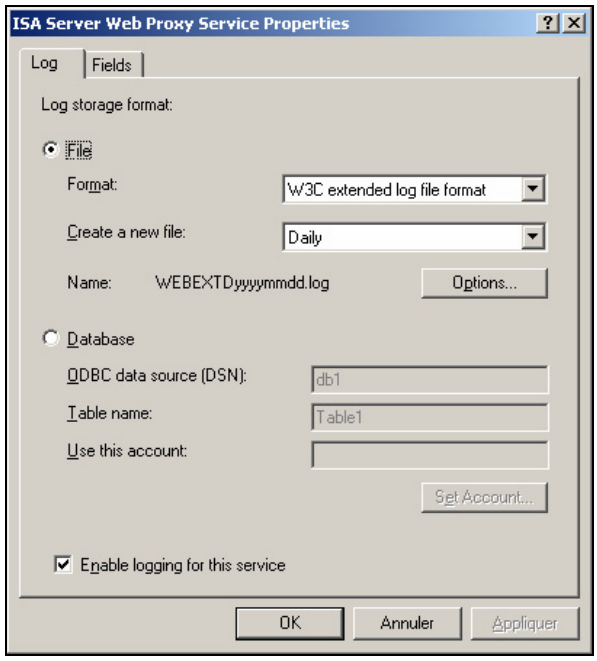
Steps

1. Right-click the applicable service in the **Details** pane.

2. Click **Properties** in the **Details** pane.

3. Right-click the applicable service.

4. Click the **File** option button in the **Log** tab.

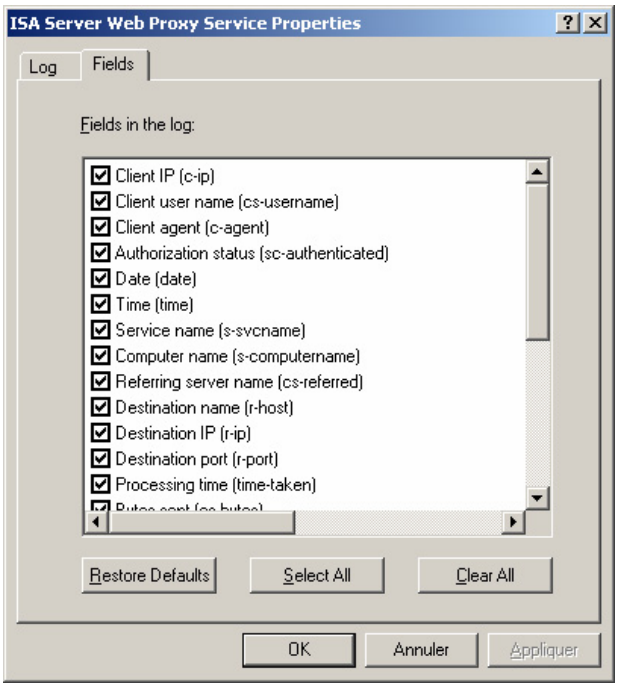


5. Enter the following information:

Format: W3C extended log file format

Create new file: select a time period that specifies how often a new log file should be created.

6. Select the Fields tab and select all the fields you want to log.



Note: W3C logs contain both data and directives describing the version, date and logged fields. Since the fields are described in the file, unselected fields are not logged. The tab character is used as a delimiter. Date and time are in GMT.

.

Section 4: Configuring Net Report Log File Analysis

4.1. Choosing a Suitable Directory

For Net Report to analyze the log file, the log files must be stored in a directory on the machine where Net Report has been installed. We recommend that the directories where the log files are stored must be local directories on the machine where Net Report is installed.

4.2. Saving Log Files from a Remote Machine

If you want to save log files from a remote machine to the machine where Net Report has been installed then files must be remotely saved in the appropriate directory on the machine where Net Report has been installed.

4.3. Saving Log Files To a Local Directory

For Net Report to analyze the log file, we recommend that the directories where the log files are stored must be local directories for that machine.

Section 5: Log Value Reference Material

This section contains the following topics:

- Action Log Values,
- Cache Info Log Values,
- Error Information Log Values,
- Operating System Log Values,
- Object Source Log Values,
- Result Code Log Values.

5.1. Introducing Result code log values

The Web Proxy and Firewall logs can include a result code field that specifies the status of the request. In the Web proxy log, this field indicates the HTTP status code. In the Firewall log, this field indicates the result code.

5.2. Understanding The Firewall Log Result Code Field Error

In the Firewall log, the result code field represents an error. It can be one of the following:

- A Windows-based HRESULT error code
- An ISA Server service error code. These errors typically begin with 0xC00. Error text typically includes FWX_E_.

5.3. Understanding The HTTP Status Code Column's http Error

The HTTP Status Code column represents an http error (from the web proxy). It can get one of the following values:

- An HTTP response code, as defined in the HTTP RFC. For a list of HTTP response codes, see the Platform SDK(http://www.microsoft.com/).
- A Winsock error code. For a list of Winsock error codes, see MSDN(http://www.microsoft.com/).
- An ISA Server Web Proxy error code. These errors also include a description.

5.4. Action Log Values

The Firewall log can include an action field. The following table lists the possible action values.

MSDE value	String in text log
0	-
1	Bind
2	Listen
3	GHBN
4	GHBA
5	Redirect-bind
6	Establish
7	Terminate
8	Denied
9	Allowed
10	Failed
11	Intermediate
12	Successful Connection
13	Unsuccessful Connection
14	Disconnection
15	User cleared Quarantine
16	Quarantine timeout

5.5. Cache Info Log Values

The Web Proxy log can include a cache info field that specifies the cache status of the object, which indicates why the object was or was not cached. The following table lists the possible cache info values.

Value	Description
0x00000001	Request should not be served from the cache.
0x00000002	Request includes the **IF-MODIFIED-SINCE** header.
0x00000004	Request includes one of these headers: **CACHE-CONTROL:NO-CACHE** or **PRAGMA:NO-CACHE**.
0x00000008	Request includes the **AUTHORIZATION** header.
0x00000010	Request includes the **VIA** header.
0x00000020	Request includes the **IF-MATCH** header.
0x00000040	Request includes the **RANGE** header.
0x00000080	Request includes the **CACHE-CONTROL: NO-STORE** header.
0x00000100	Request includes the CACHE-CONTROL: MAX-AGE, CACHE-CONTROL: MAX-STALE, or CACHE-CONTROL: MIN-FRESH header.
0x00000200	Cache could not be updated.
0x00000400	**IF-MODIFIED-SINCE** time specified in the request is newer than cached **LASTMODIFIED** time.
0x00000800	Request includes the **CACHE-CONTROL: ONLY-IF-CACHED** header.
0x00001000	Request includes the **IF-NONE-MATCH** header.
0x00002000	Request includes the **IF-UNMODIFIED-SINCE** header.
0x00004000	Request includes the **IF-RANGE** header.
0x00008000	More than one **VARY** header.

0x00010000	Response includes the **CACHE-CONTROL: PUBLIC** header.
0x00020000	Response includes the **CACHE-CONTROL: PRIVATE** header.
0x00040000	Response includes the CACHE-CONTROL: NO-CACHE or PRAGMA: NO-CACHE header.
0x00080000	Response includes the **CACHE-CONTROL: NO-STORE** header.
0x00100000	Response includes either the CACHE-CONTROL: MUST-REVALIDATE or CACHE-CONTROL: PROXY-REVALIDATE header.
0x00200000	Response includes the **CACHE-CONTROL: MAX-AGE** or **S-MAXAGE** header.
0x00400000	Response includes the **VARY** header.
0x00800000	Response includes the **LAST-MODIFIED** header.
0x01000000	Response includes the **EXPIRES** header.
0x02000000	Response includes the **SET-COOKIE** header.
0x04000000	Response includes the **WWW-AUTHENTICATE** header.
0x08000000	Response includes the **VIA** header.
0x10000000	Response includes the **AGE** header.
0x20000000	Response includes the **TRANSFER-ENCODING** header.
0x40000000	Response should not be cached.

5.6. Error Information Log Values

The Web Proxy log can include an error information field. The following table lists the possible values.

MSDE value	Description
0x00000001	Error receiving packets from client
0x00000002	Error sending packets to client
0x00000004	Error sending packets to server
0x00000008	Error receiving packets from server
0x00000040	Error while connecting
0x00000080	Connection with client is "Keep-Alive"
0x00000100	Connection with upstream server is "Keep-Alive"
0x00000200	Client's request includes a body (of non-zero content length)
0x00000400	Server's response includes a body (of non-zero content length)
0x00000800	Name resolution made using DNS cache

5.7. Operating System Log Values

The Web Proxy and Firewall logs can include a Client Agent field that specifies the operating system initiating the request. The following table lists the possible operating system values.

Value	Description
0:3.1	Windows® 3.1
0:3.11	Windows for Workgroups
0:3.95	Windows 95 (16-bit)
1:3.11	Win32s
2:4.0	Windows 95 (32-bit)
2:4.10	Windows 98
2:4.90	Windows Millennium Edition
3:3.1	Windows NT® 3.1
3:3.5	Windows NT 3.5
3:3.51	Windows NT 3.51
3:4.0	Windows NT 4.0
3:5.0	Windows 2000
3:5.1	Windows XP
3:5.2	Windows Server™ 2003

If ISA Server does not recognize the operating system, the log field value is set to Unknown

5.8. Object Source Log Values

The Web Proxy log can include an object source field that specifies the source that was used to retrieve the current object. For more information, see Log viewer and Web Proxy log fields. The following table lists the possible object source values.

Source values	String in text log	Description
0	(None)	No source information is available.
1	Cache	Source is the cache. Object returned from cache.
2	Verified Cache	Source is the cache. Object was verified to source and had not been modified.
3	Not Verified Cache	Source is the cache. Object could not be verified to source.
4	Verify Failed Internet	Source is the Internet. The object in the cache was not valid, and was retrieved from the Internet.
5	Internet	Source is the Internet. Object added to cache.
7	Upstream	Object returned from an upstream proxy cache.
8	Not Modified	Source is the cache. Client performed an If-Modified-Since request and object had not been modified.

Section 6: Settings Reference Material

6.1. Default Settings

After installation, ISA Server uses the default settings that are listed in the following table.

Feature	Default Setting
User permissions	Members of the Administrators group on the local computer can configure firewall policy.
Network settings	The following network rules are created: **Local Host Access.** Defines a routed network relationship between the Local Host network and All Networks. This essentially defines a network relationship for services running on the ISA Server computer to other networks. **Internet Access.** Defines a NAT network relationship from the Internal network, the Quarantined VPN Clients network, and the VPN Clients network, to the External network. Access will be allowed only if you configure the appropriate access policy. **VPN Clients to Internal Network.** Defines a routed network relationship between the VPN Clients network and the Internal network. Access will be allowed only if you enable VPN client access.
Access rules	The following default rules are created: **Default rule.** This rule denies all traffic between all networks. **System policy rules.** A series of rules such that ISA Server can interact with other network resources.
Publishing	No internal servers are accessible to external clients.
Web routing	**Default Rule.** This rule specifies that all Web Proxy client requests are retrieved directly from the Internet.
Caching	The cache size is set to 0. All caching is therefore disabled.

6.2. New Ways To Do Familiar Tasks

The following table lists common tasks you can perform using ISA Server Preview and compares these tasks to how they were performed using ISA Server 2000.

If you want to	In ISA Server 2000	In ISA Server Preview
Publish co-located servers.	Create a static packet filter allowing access to the specific server located on the ISA Server computer.	Create a server publishing rule.
Enable an application on the ISA Server computer to access the Internet.	Create a static packet filter allowing access to the specific port on the ISA Server computer.	Verify that the default network rule, which is created upon installation, accurately defines a relationship between the Local Host network and the External network. Then, create an access rule that allows access to the specific protocol.
Configure the local address table (LAT).	Click **Local Address Table** on any service's properties.	The Internal network replaces the local address table, and is configured as part of the setup process. You can subsequently reconfigure the Internal network.
Configure IP-based protocol support.	ISA Server supported IP-based protocols in a limited fashion.	Create a protocol definition, specifying any of the following protocols: TCP, UDP, ICMP, or IP-level. If you select IP-level, you can specify any low-level protocol.
Configure virtual private networking.	Use the VPN wizards to configure VPN.	Enable VPN client access and configure the VPN properties.
Configure outgoing Web request properties.	On the array properties, click the **Outgoing Web requests** tab and configure listener properties.	Each network has its own listener, the network adapter that is responsible for listening for requests bound for that network.
Configure incoming Web request properties.	On the array properties, click the **Incoming Web requests** tab and configure listener	Web listeners are used as part of each Web publishing rule. When you configure a Web publishing rule, you specify which Web listener to use for

	properties.	that rule.

Contacting Net Report

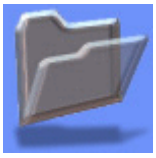
For Technical Support, please contact us:

By e-mail at: support@netreport.fr

By Telephone on: +33 (0)46 784 4800

By Fax on: +33 (0)46 784 4811

By post at: Net Report Headquarters,
130 rue Baptistou,
ZAE Nord,
34980 Saint Gély du Fesc,
France



For Sales Enquiries, please contact us:

By Telephone on: +33 (0)1 46 84 15 66

By post at: Net Report Sales Offices,
Allasso France,
Immeuble Europe Avenue,
3ème et 4ème étage (Reception),
62 Bis av André Morizet,
92 643 Boulogne-Billancourt Cedex,
FRANCE