

The Winfrasoft XFF logo consists of the word "Winfrasoft" in a small, blue, sans-serif font, followed by the letters "XFF" in a large, bold, blue, sans-serif font. A blue swoosh or arc is positioned below the "XFF" letters.

X-Forwarded-For for IIS

Installation and configuration guide

Full X-Forwarded-For support for Microsoft Internet Information Server 10

Published: June 2026
Applies to: Winfrasoft X-Forwarded-For for IIS 2.0.4
Web site: <https://winfrasoft.com>
Email: support@winfrasoft.com

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organisations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organisation, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

Winfrasoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written licence agreement from Winfrasoft, the furnishing of this document does not give you any licence to these patents, trademarks, copyrights, or other intellectual property.

Microsoft, Active Directory, Windows and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

TABLE OF CONTENTS	3
INTRODUCTION	4
CONSIDERATIONS	4
<i>Server System Requirements</i>	4
<i>Language Requirements</i>	4
LICENSING	5
<i>Running a trial</i>	5
X-FORWARDED-FOR AND SECURITY	6
BACKGROUND	6
INTEROPERABILITY WITH PROXY SERVERS	6
WEB SERVER SECURITY	6
DESIGN AND DEPLOYMENT SCENARIOS	8
ANTI-SPOOFING PROXY TRUST LIST TECHNOLOGY	8
SCENARIO #1 – NO PROXY TRUST LIST CONFIGURED	8
SCENARIO #2 – PROXY TRUST LIST CONFIGURED	9
DEPLOYMENT	12
OVERVIEW	12
INSTALLING X-FORWARDED-FOR FOR IIS	13
UNINSTALLING X-FORWARDED-FOR FOR IIS	15
CONFIGURATION REVIEW	18
<i>IIS 6.0 on Windows Server 2003</i>	18
<i>IIS 7.0 on Windows Server 2008</i>	20
<i>IIS 7.0 and ISAPI Site Inheritance</i>	21
RUNNING A 32BIT WEB SITE ON A 64BIT SERVER	22
<i>Server level</i>	22
<i>Site level</i>	22
<i>Setting the App Pool to 32bit mode</i>	24
CONFIGURING A PROXY TRUST LIST	25
ADDITIONAL INFORMATION	26
“HOW TO” GUIDES	26
SUPPORT GUIDES	26

Introduction

X-Forwarded-For for IIS is an ISAPI web filter that integrates with Microsoft Internet Information Server (IIS) to:-

- Modify the “c-ip” field in the IIS logs with the first non-trusted client IP address detected within the X-Forwarded-For HTTP header (see Configuring a Proxy Trust List), or
- Modify the “c-ip” field in the IIS logs with the full X-Forwarded-For HTTP header list together with the actual layer 4 IP source to track the entire chain.
- Support both HTTP and HTTPS traffic for reverse proxy deployments. HTTPS functionality is reliant on a SSL certificate being installed on the web server.
- Integrate with other 3rd party products that support the X-Forwarded-For de facto standard.



Note

By default, the IIS Default Web Site log files are located in the `C:\Windows\System32\LogFiles\W3SVC1\` folder.

Considerations

Server System Requirements

The minimum system requirements for X-Forwarded-For for IIS are:

- x64 systems with Windows Server 2016 and higher
- Microsoft Internet Information Server 10

Language Requirements

Server

X-Forwarded-For for IIS is compatible with multi-lingual versions of Windows, however is only available in English. Product support and documentation is only available in English.

Licensing

X-Forwarded-For for IIS is licensed on a per server basis. A licence file must be installed onto each Internet Information Server otherwise the application will function in trial mode.

To install a Winfrasoft X-Forwarded-For for IIS licence file, simply copy the supplied licence file (XFF4IIS.lic) into the application installation folder of the server which requires a licence. The default installation folder is:

```
C:\Program Files\Winfrasoft X-Forwarded-For for IIS\
```



Note

For detailed information on the licence types please refer to the licence agreement document included within the installation program.

Running a trial

When Winfrasoft X-Forwarded-For for IIS is first installed it will operate in a demo/lab mode. The demo/lab mode is fully functional for 14 days, after which the filter will cease to operate. Once it has expired, Microsoft IIS will continue to function as though X-Forwarded-For for IIS was not installed.

X-Forwarded-For and Security

Background

Historically there have been many security flaws with systems that support the X-Forwarded-For HTTP header. Many implementations fell victim to spoof attacks where systems were given spoofed X-Forwarded-For information and they inadvertently processed a rule or action based on this information.

X-Forwarded-For IP information is clear text inside a HTTP header; it is NOT signed and is NOT authenticated. This can pose a huge security risk if allow and deny security decisions are made based on the data stored in the X-Forwarded-For header especially if the data originates from the Internet.

Another historic security issue with the technology is that internal IP address information could be revealed to the Internet, which could unwittingly divulge information about the internal infrastructure.

There is no RFC or official standard for X-Forwarded-For and as such many vendors implemented their own version of X-Forwarded-For in their products which lead to some incompatibilities, although many have since been resolved. The X-Forwarded-For methodology used in Squid and other big brands, such as F5 and Bluecoat, have become the de facto standard. This lack of standards is why Microsoft has not implemented X-Forwarded-For support natively in IIS. Different vendors implement X-Forwarded-For in different ways, as such, Winfrasoft cannot guarantee interoperability with other vendors although our implementation is as generic as possible for maximum compatibility.

Interoperability with Proxy Servers

Winfrasoft X-Forwarded-For for IIS has been fully tested and is supported to interoperate with reverse web proxy chain scenarios.

Reverse Proxy Traffic

It is critical when using X-Forwarded-For for inbound traffic to verify the entire X-Forwarded-For IP list to ensure that trusted IP addresses are listed before the original client IP to avoid spoofing in logs.

Web Server Security

When logging the original client IP address on a web server, the entire X-Forwarded-For list together with the layer 4 source IP should be verified to ensure that the first IP address that is not trusted is used, and not just the first IP address in the list. This will help to remove the risk of inadvertently logging spoofed IP addresses for the original client IP.

Given the following X-Forwarded-For list received by a Web Server where xxx.xxx.xxx.xxx is an invalid/spoofed IP address, yyy.yyy.yyy.yyy is the IP address of the machine that connected to the Internet proxy and zzz.zzz.zzz.zzz is the IP address of the Internet proxy

server. The web server would receive a layer 4 routable IP connection from `zzz.zzz.zzz.zzz` containing the following X-Forwarded-For header as follows...

X-Forwarded-For: `xxx.xxx.xxx.xxx`, `yyy.yyy.yyy.yyy`

Layer 4 routable source IP: `zzz.zzz.zzz.zzz`

In this case, a security conscious Web Server could be configured to know that `zzz.zzz.zzz.zzz` is a trusted proxy server and thus `yyy.yyy.yyy.yyy` is the first foreign IP Address. As such the Web Server should determine that `yyy.yyy.yyy.yyy` is the actual original client IP address and the `xxx.xxx.xxx.xxx` entry should be ignored.



Warning!

Many IIS based X-Forwarded-For filters simply log the first IP address in the X-Forwarded-For list which may not always be the correct value. Others only log the X-Forwarded-For field and not the layer 4 routable source IP address losing part of the chain information.

Winfrasoftware X-Forwarded-For for IIS uses Proxy Trust List technology as described above or can log the entire proxy chain list.

Design and Deployment Scenarios

Winfrasoft X-Forwarded-For for IIS has been designed to suite the following security and logging scenarios. The product may function in other scenarios too however Winfrasoft is unable to test every combination, especially with 3rd party products which also support X-Forwarded-For. It is recommended that all deployment scenarios are tested in a lab prior to a live deployment.

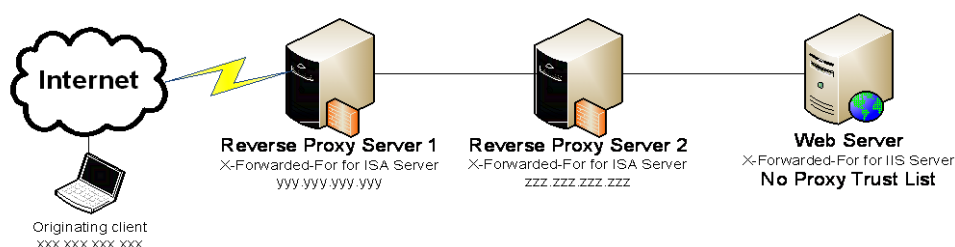
Anti-Spoofing Proxy Trust List technology

An Anti-Spoofing proxy trust list can be created to determine which IP address from the X-Forwarded-For HTTP header is reflected in the IIS “c-ip” log field. The purpose of the proxy trust list is to specify the IP addresses of internal servers in a proxy chain so the web server can correctly log the first un-trusted IP address as the real Internet client. This technology is designed to prevent spoofed IP addresses from poisoning your web server log information.

The proxy trust list is contained in the XFF4IIS.INI file located in the installation folder. If the trust list is empty or the file does not exist then X-Forwarded-For for IIS will log the entire X-Forwarded-For list together with the layer 4 source IP address of the closest proxy server so that the “c-ip” field contains a complete chain list.

Scenario #1 – No Proxy Trust List Configured

This scenario describes the functionality of X-Forwarded-For for IIS in an environment with 2 reverse proxy servers, with X-Forwarded-For support, configured for web publishing. More than two reverse proxy servers can be used in a chain. A mixture of technologies is also supported, e.g. F5 hardware load balancing device. This example will assume that two reverse proxies are used.



The Web Server is responsible for processing the X-Forwarded-For header information that is received from the last proxy server. As there is no proxy trust list configured all the IP addresses in the X-Forwarded-For header will be logged together with the IP address of the closest proxy server.

Server

Reverse Proxy Server 1 “X-Forwarded-For” field does not exist in header of HTTP Request	Reverse Proxy adds the “X-Forwarded-For” field containing the Internet original client IP address to the HTTP header of a request when Web Publishing to Reverse Proxy Server 2. Header syntax where xxx.xxx.xxx.xxx is the Internet original client IP address: <pre>X-Forwarded-For: xxx.xxx.xxx.xxx</pre>
Reverse Proxy Server 2	Append the IP address of Proxy Server 1 to the “X-Forwarded-For” field which already contains the Internet original client IP address to the HTTP header of a HTTP request when Web Publishing to the Web server. Header syntax received by the Web Server where xxx.xxx.xxx.xxx is the Internet original client IP address and yyy.yyy.yyy.yyy is the IP address of Proxy Server 1: <pre>X-Forwarded-For: xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy</pre>
Web Server “X-Forwarded-For” field exists in header of HTTP Request	Winfrasoft X-Forwarded-For for IIS will first assemble the entire X-Forwarded-For header and the IP address of the last proxy server in the web proxy chain into a <i>Proxy Chain List</i>. Next, as there is no Proxy Trust List, the entire <i>Proxy Chain List</i> is logged within the “c-ip” (Client source) IIS log field. From this, the full path to the web server can be determined. Note: The IP address of the last proxy server in the web proxy chain is not contained within the actual X-Forwarded-For header. <pre>Proxy Trust list: (empty) X-Forwarded-For: xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy Layer 4 source IP: zzz.zzz.zzz.zzz Proxy Chain List: xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy, zzz.zzz.zzz.zzz</pre> Resulting c-ip value: xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy, zzz.zzz.zzz.zzz Example W3C Log file result: <pre>#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs (User-Agent) sc-status sc-substatus sc-win32-status 2008-09-07 14:37:03 W3SVC1 192.168.0.1 GET /Default.htm - 80 - xxx.xxx.xxx.xxx,+yyy.yyy.yyy.yyy,+zzz.zzz.zzz.zzz Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+.NET+CLR+2.0.50727) 200 0 0</pre>

**Note**

As a W3C file is space delimited a field entry can not contain spaces, thus any spaces are automatically be replaced by a “+” character by IIS.

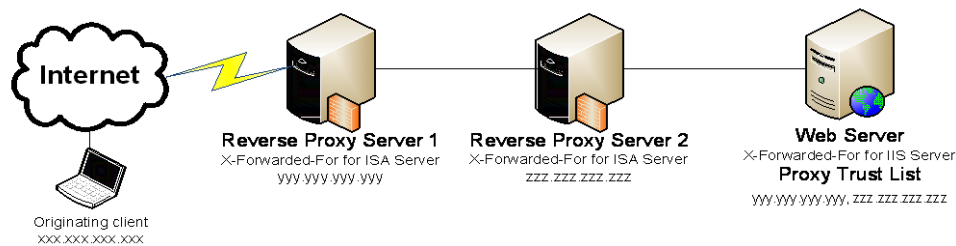
Scenario #2 –Proxy Trust List Configured

This scenario is the same as Scenario 1 except that a Proxy Trust List has been configured.

The Web Server is responsible for processing the X-Forwarded-For header information that is received. Microsoft IIS does not support X-Forwarded-For natively and requires Winfrasoft X-Forwarded-For for IIS to log the original client IP address on the Web Server from information received in the X-Forwarded-For header.

In this scenario, Reverse Proxy 1 and Reverse Proxy 2 are both trusted, as such the proxy trust list configuration file (XFF4IIS.INI) would appear as :

```
[Config]
TrustList=yyy.yyy.yyy.yyy, zzz.zzz.zzz.zzz
```



Server	
Reverse Proxy Server 1 “X-Forwarded-For” field does not exist in header of HTTP Request	Reverse Proxy adds the “X-Forwarded-For” field containing the Internet original client IP address to the HTTP header of a request when Web Publishing to Reverse Proxy Server 2. Header syntax where xxx.xxx.xxx.xxx is the Internet original client IP address: X-Forwarded-For: xxx.xxx.xxx.xxx
Reverse Proxy Server 2	Append the IP address of Proxy Server 1 to the “X-Forwarded-For” field which already contains the Internet original client IP address to the HTTP header of a HTTP request when Web Publishing to the Web server. Header syntax received by the Web Server where xxx.xxx.xxx.xxx is the Internet original client IP address and yyy.yyy.yyy.yyy is the IP address of Proxy Server 1: X-Forwarded-For: xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy

Web Server “X-Forwarded-For” field exists in header of HTTP Request	Winfrasoft X-Forwarded-For for IIS will first assemble the entire X-Forwarded-For header and the IP address of the last proxy server in the web proxy chain into a <i>Proxy Chain List</i>. Next, each IP address in the <i>Proxy Chain List</i> will be compared with each IP address on the Proxy Trust List. Parsing of the <i>Proxy Chain List</i> is performed from right to left effectively starting with the IP address closest to the web server. The first IP address found to be un-trusted is assumed to be the real Internet client IP address as this was the IP address which established a routed connection to the last trusted proxy server closest to the Internet. Therefore, the closest non-trusted IP address will appear in the “c-ip” field as the real client source IP address. Proxy Trust list: <code>yyy.yyy.yyy.yyy, zzz.zzz.zzz.zzz</code> X-Forwarded-For: <code>xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy</code> Layer 4 source IP: <code>zzz.zzz.zzz.zzz</code> Proxy Chain List: <code>xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy, zzz.zzz.zzz.zzz</code> Resulting c-ip value: <code>xxx.xxx.xxx.xxx</code> Example W3C Log file result: <pre>#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status 2008-09-07 14:37:03 W3SVC1 192.168.0.1 GET /Default.htm - 80 - xxx.xxx.xxx.xxx Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+.NET+CLR+2.0.50727) 200 0 0</pre>
--	---



Note

As a W3C file is space delimited a field entry can not contain spaces, thus any spaces are automatically be replaced by a “+” character by IIS.

If **all IP addresses** in the Proxy Chain List are deemed to be trusted then the **last IP address** will be logged in the “c-ip” field. e.g. `xxx.xxx.xxx.xxx`.

If **no IP addresses** in the Proxy Chain List are deemed to be trusted then the **first IP address** will be logged in the “c-ip” field. e.g. `zzz.zzz.zzz.zzz`.

Deployment

Overview

This deployment section assumes that the Web Proxy chain has been established and the web pages within IIS have been correctly published and tested.



Note

This guide does not detail how to establish reverse proxy servers or how to publish web pages using IIS. See the proxy product documentation from your vendor or Microsoft documentation on publishing web pages on IIS.

To fully deploy the X-Forwarded-For for IIS solution the following steps must be performed:

- (1) Deploy and configure IIS services & site content and test functionality
- (2) Deploy and configure a reverse proxy solution which supports X-Forwarded-For and test functionality
- (3) Verify traffic using a network sniffer like Network Monitor (where SSL is not being used) to ensure that X-Forwarded-For data is being received on the web server.
- (4) Install X-Forwarded-For for IIS on the web server.
- (5) Check the IIS logs and verify the IP addresses listed as the originating client address ('c-ip' field)

Installing X-Forwarded-For for IIS

When X-Forwarded-For for IIS is first installed, the setup routine will, by default, register and enable the web filter within Internet Information Server. No IIS Services require a restart to activate X-Forwarded-For IIS ISAPI web filter.

X-Forwarded-For for IIS is installed under the global Web Sites section of the IIS MMC and will apply to ALL web sites defined on the server.

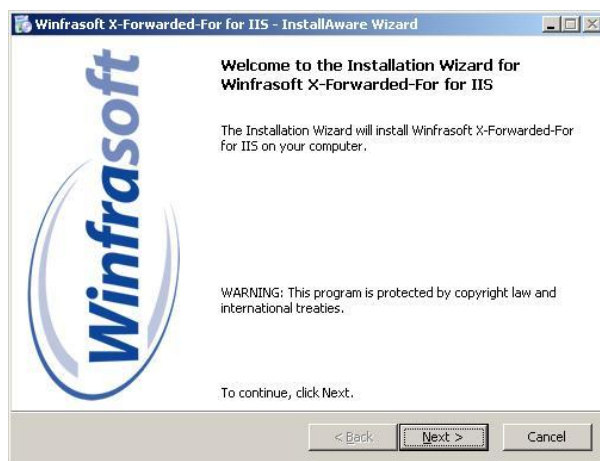


Note

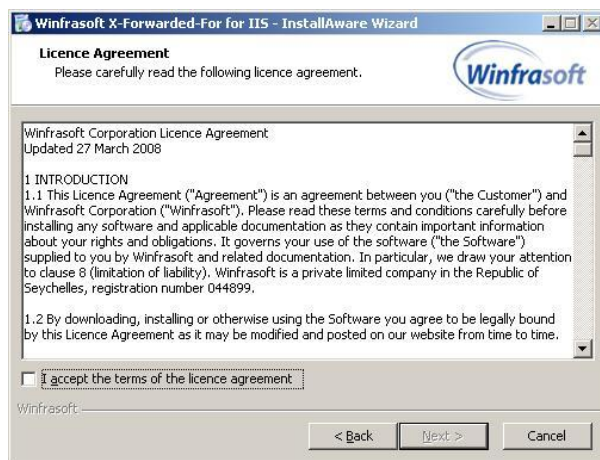
When installing X-Forwarded-For for IIS on Windows Server 2008 please ensure that the **IIS 6 Metabase Compatibility** Role Service has been installed.

See <http://www.winfrasoft.com/kb-28.htm> for further information.

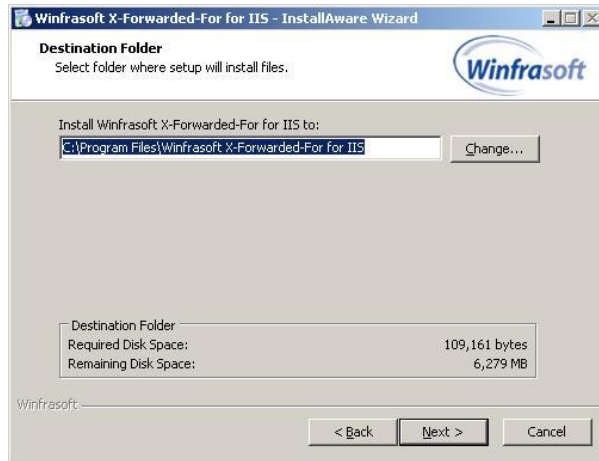
- (1) To start the X-Forwarded-For for IIS installation execute the *XFFforIIS2.0.exe* installer package.
- (2) This starts the setup wizard:



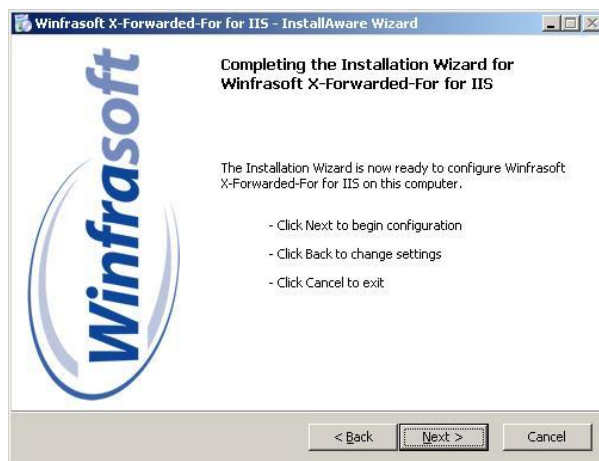
- (3) Click *Next* to continue.



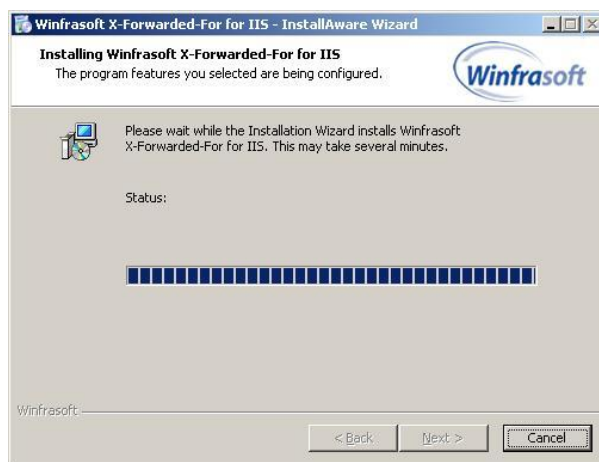
- (4) After reading the licence agreement click *I accept the terms in the terms in the License Agreement* if you agree to the terms, then click *Next* to continue.



- (5) Select the destination for the install and Click *Next* to continue.



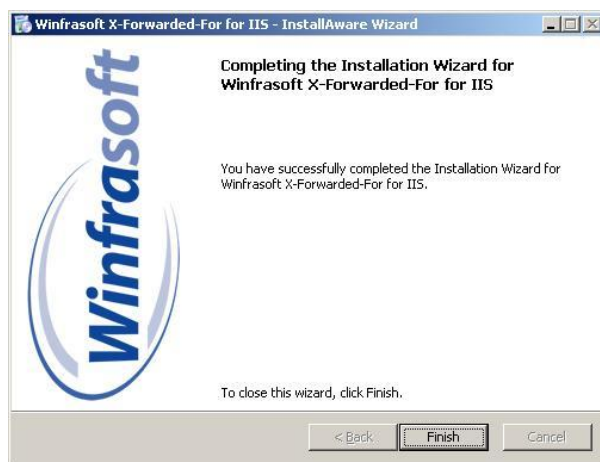
- (6) Click *Next* to continue.



The installation files are copied and the ISAPI filter registered in IIS.



- (7) Click *OK* to continue.

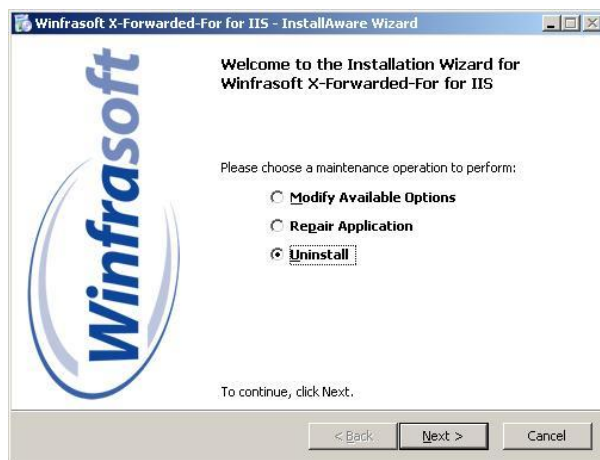


- (8) Click *Finish* to complete the installation process.

Uninstalling X-Forwarded-For for IIS

If you no longer require X-Forwarded-For for IIS to be installed you and remove it from a server as follows:

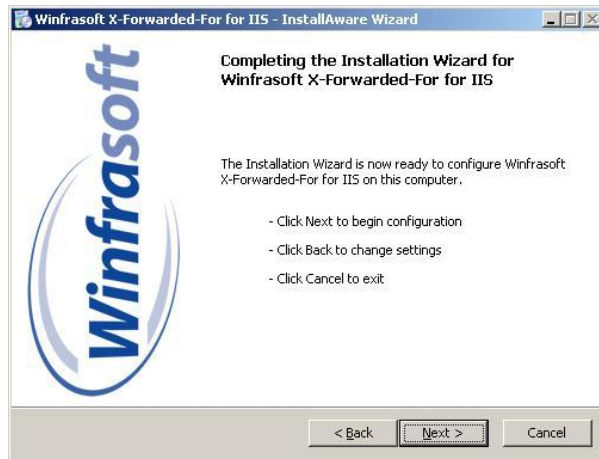
- (1) To start the X-Forwarded-For for IIS un-installation, on a server where X-Forwarded-For for IIS has been previously installed, execute the *XFFforIIS2.0.exe* installer package. Alternatively use Add/Remove Programs in the Control Panel and click Remove.
- (2) Running the executable file starts the setup wizard.



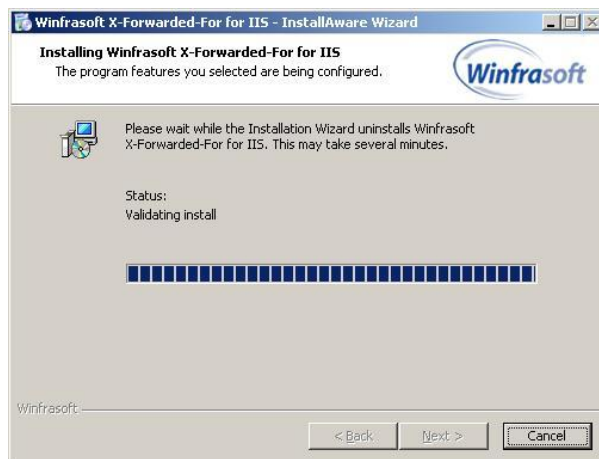
**Note**

As with the installation process, no IIS services require a restart to disable the X-Forwarded-For for IIS ISAPI filter.

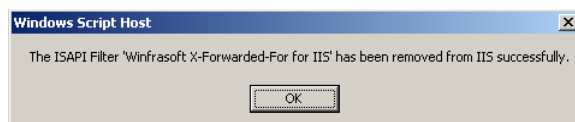
- (3) Select *Uninstall* and Click *Next* to continue.



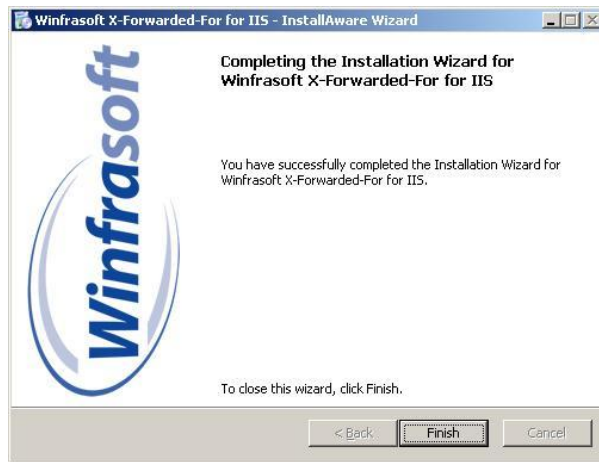
- (4) Click *Next* to continue.



The ISAPI filter is deregistered from IIS and installation files are removed.



- (5) Click *OK* to continue.



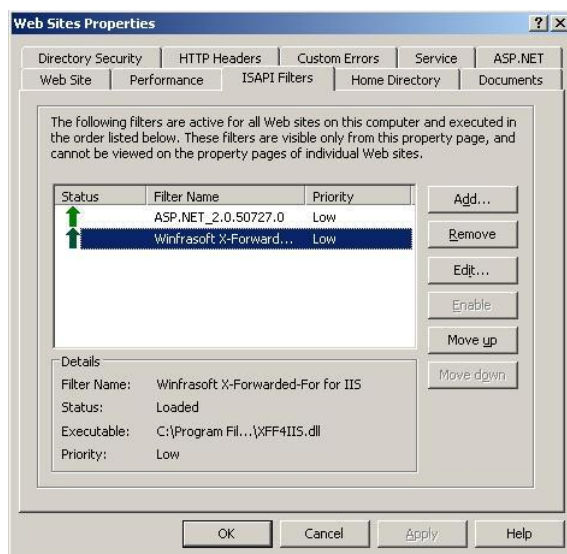
(6) Click *Finish* to complete un-installation.

Configuration review

Winfrasoft X-Forwarded-For for IIS modifies the “c-ip” field within IIS log files. IIS logging is configured via the Properties Tab of all web sites, or each individual web site, in the Internet Information Services Manager.

IIS 6.0 on Windows Server 2003

After the installation of X-Forwarded-For for IIS, the ISAPI filter registration will be visible in the Web Site Properties window on the *ISAPI Filters* tab of the IIS Management console as follows:

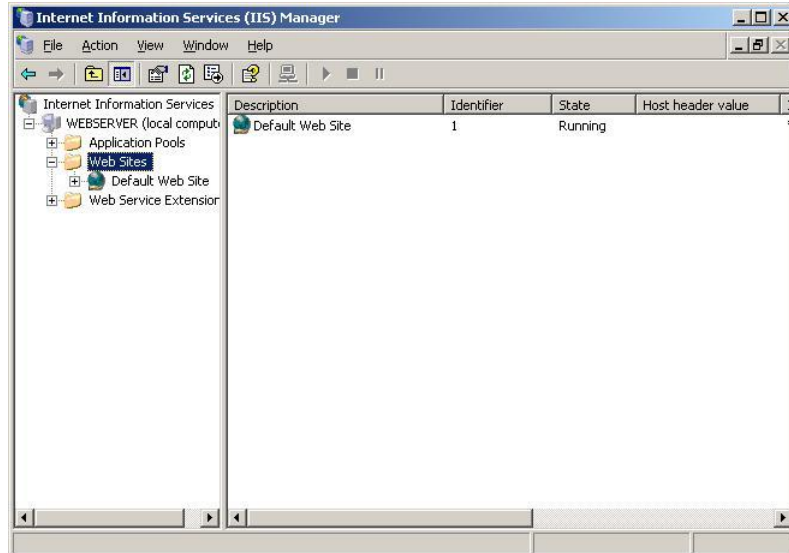


Note

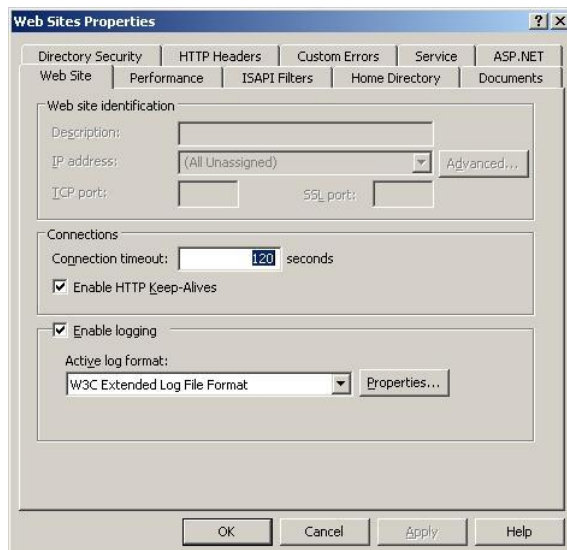
X-Forwarded-For for IIS ISAPI Filter can be moved up and down in the priority list through the IIS Management console.

To ensure IIS logging is enabled

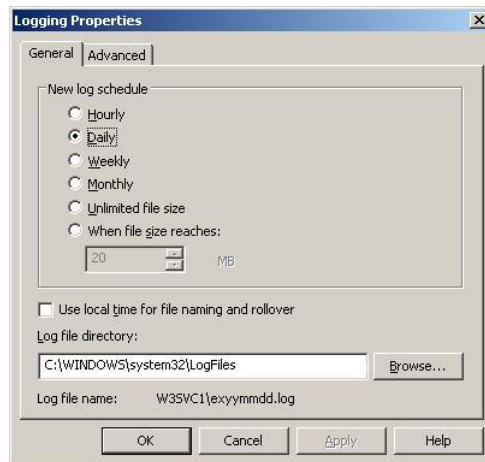
- (1) Right click *Web Sites* and select *Properties*.



- (2) Ensure that *Enable logging* is checked.



- (3) Click *Properties* to check and/or change the folder location of your IIS Log files if required.



(4) Click *OK*, and *OK* again to close.

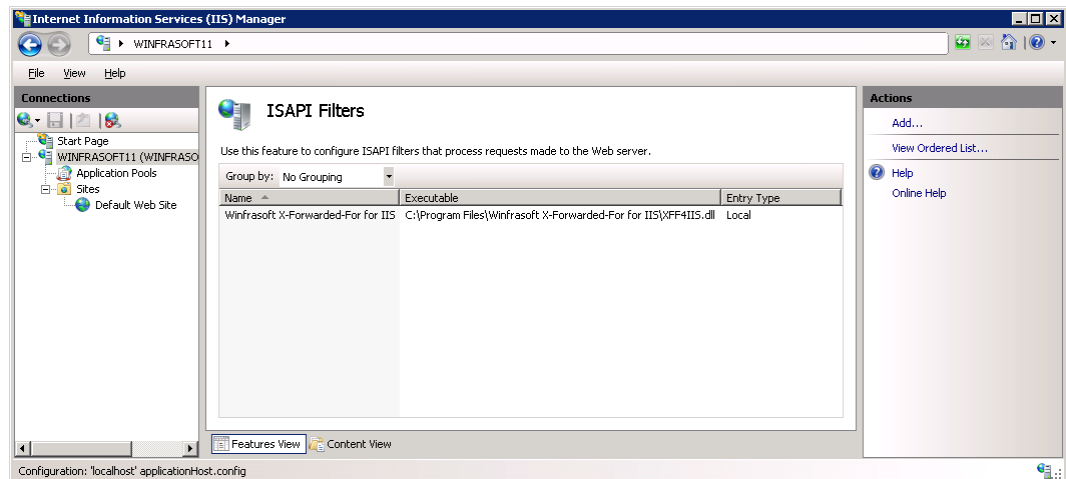


Note

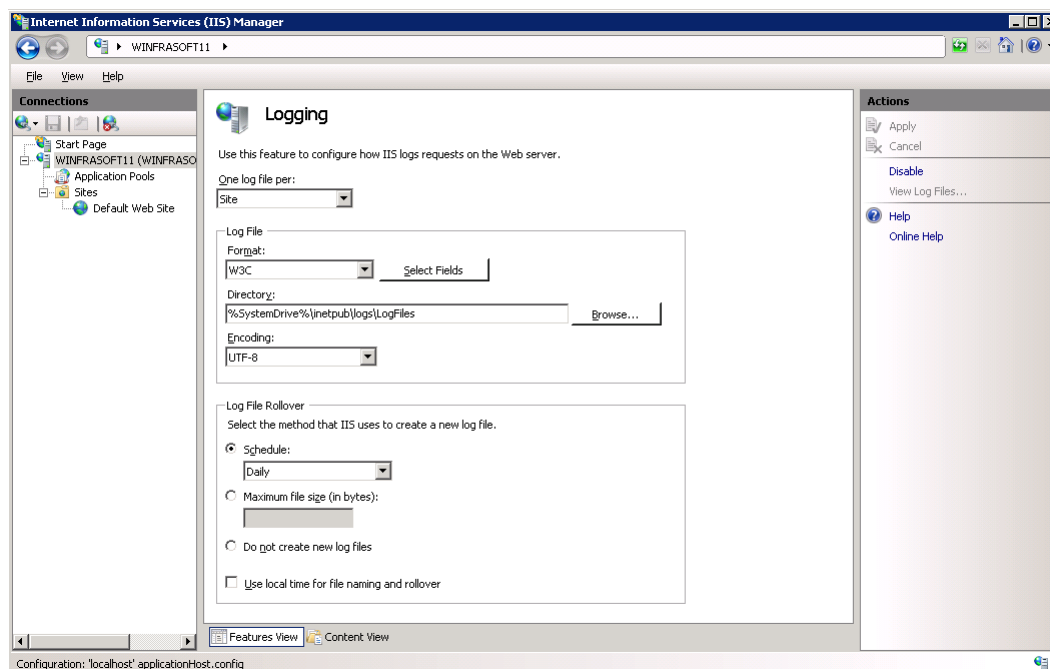
The X-Forwarded-For ISAPI filter can be enabled or disabled on each configured web site through the IIS Management Console. There is no user interface required for X-Forwarded-For for IIS.

IIS 7.0 on Windows Server 2008

After the installation of X-Forwarded-For for IIS, the ISAPI filter registration will be visible in the *ISAPI Filters* section of the IIS Management console as follows:



To ensure IIS logging is enabled select *Logging* section of the IIS Management console.



Check and/or change the folder location of your IIS Log files if required.



Note

The X-Forwarded-For ISAPI filter can be enabled or disabled on each configured web site through the IIS Management Console. There is no user interface required for X-Forwarded-For for IIS.

IIS 7.0 and ISAPI Site Inheritance

Unlike IIS6, IIS7 supports both Global and Site based ISAPI filters. By default a web site will inherit the Global ISAPI filter list (where X-Forwarded-For for IIS is registered), but if inheritance is disabled then X-Forwarded-For for IIS will no longer function on the web site.

To allow X-Forwarded-For for IIS to function on a web site that *does not* allow inheritance of ISAPI filters you need to manually register the X-Forwarded-For for IIS ISAPI filter with the web site.

See <http://www.winfrasoft.com/kb-27.htm> for further information.

Running a 32bit Web Site on a 64bit server

The X-Forwarded-For for IIS installation program will install both the x86 and x64 files when a installed on a 64bit server, however only the x64 version will be registered in IIS.

Server level

The x86 ISAPI filter can be installed at the server level in IIS which takes effect on all web sites/worker pools which inherit their settings from the server. This should only be done if all the web sites/worker pools on the server run as a 32bit process, or any 64bit web sites/worker pools do not inherit ISAPI settings from the server level.

A script which will uninstall the x64 ISAPI filter and install the x86 ISAPI filter on a 64bit server at the IIS ROOT level is located in the application installation directory at:

```
C:\Program Files\Winfrasoft X-Forwarded-For for IIS\instx86.cmd
```



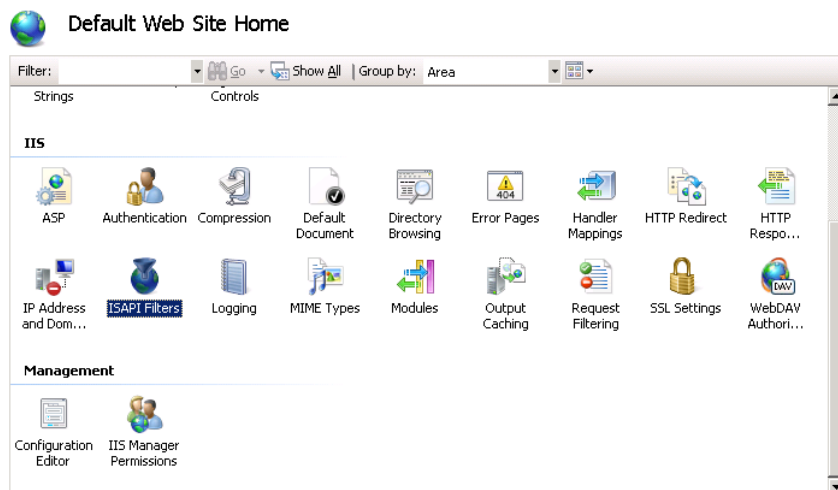
Note

The instx86.cmd script MUST be run from a command prompt with Elevated Administrator rights.

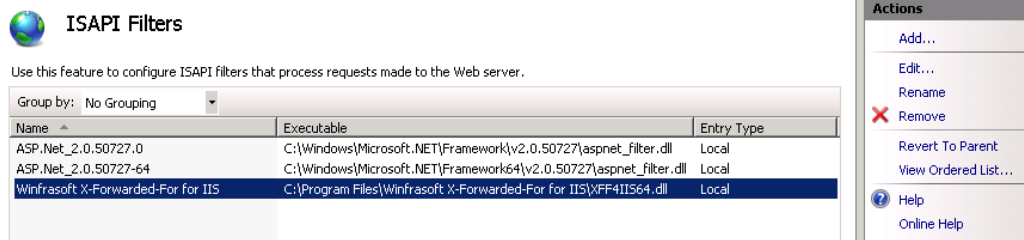
Site level

If you have a web site/worker pool which is required to run as a 32bit process then you will need to remove the x64 ISAPI filter from that web site (not necessarily the web server) and add the x86 ISAPI filter reference instead. This must be done manually as follows:

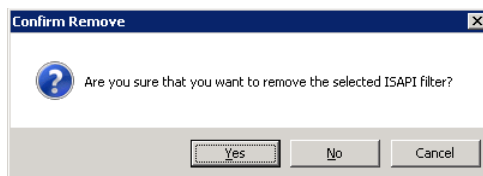
- (1) Open the IIS Manager and select the required web site. Ensure “Features View” is enabled.



- (2) Double click the *ISAPI Filters* icon.
- (3) Select the *Winfrasoft X-Forwarded-For for IIS* filter.



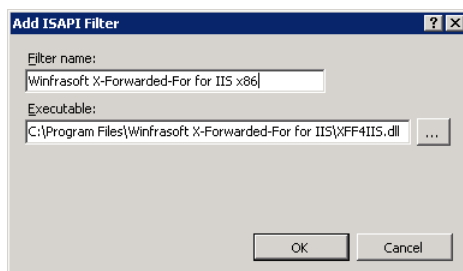
- (4) Ensure the that DLL file name selected is XFF4IIS64.DLL and click *Remove*.



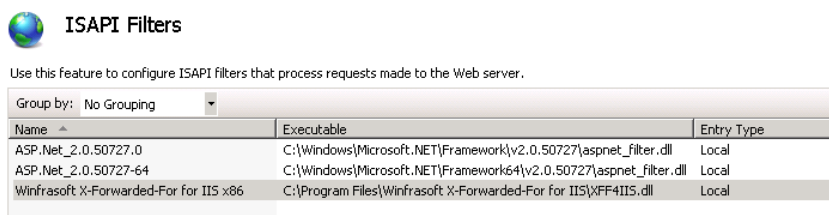
- (5) Click *Yes* to confirm.

- (6) Click *Add...*

- (7) Enter Winfrasoft X-Forwarded-For for IIS x86 in the filter name box and C:\Program Files\Winfrasoft X-Forwarded-For for IIS\XFF4IIS.dll in the executable box and click OK.



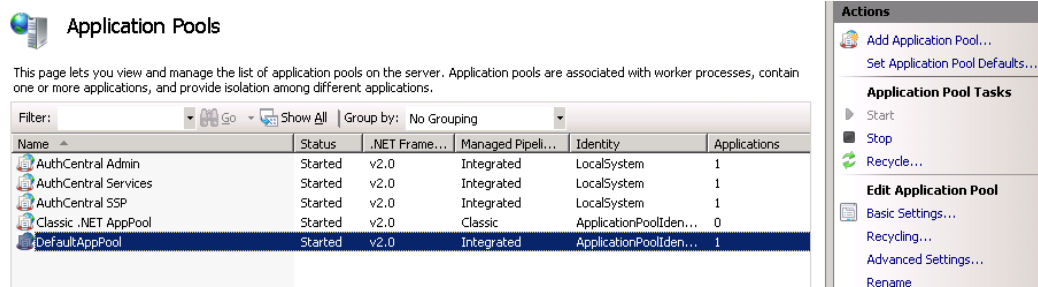
- (8) The 32bit ISAPI filter is now added.



Setting the App Pool to 32bit mode

You must ensure that the Application Pool for the web site is set to run in 32bit mode otherwise the filter will fail to load:

- (1) Select the App Pool



Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Filter: [v] Go [v] Show All [v] Group by: No Grouping [v]

Name	Status	.NET Frame...	Managed Pipeli...	Identity	Applications
AuthCentral Admin	Started	v2.0	Integrated	LocalSystem	1
AuthCentral Services	Started	v2.0	Integrated	LocalSystem	1
AuthCentral SSP	Started	v2.0	Integrated	LocalSystem	1
Classic .NET AppPool	Started	v2.0	Classic	ApplicationPoolIden...	0
DefaultAppPool	Started	v2.0	Integrated	ApplicationPoolIden...	1

Actions

- Add Application Pool...
- Set Application Pool Defaults...

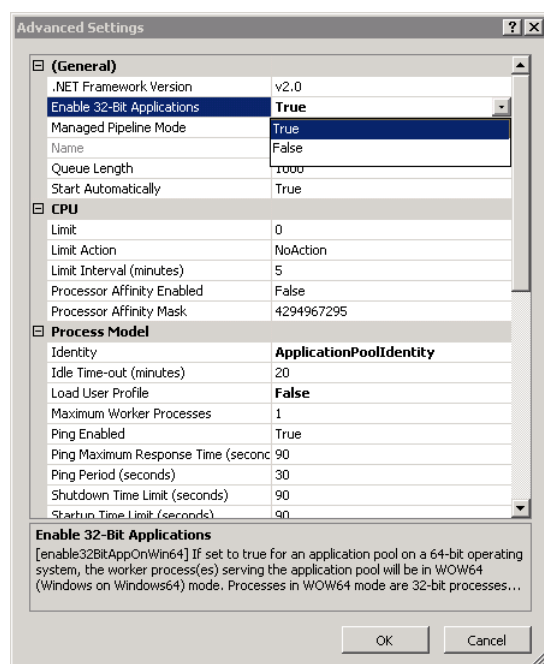
Application Pool Tasks

- Start
- Stop
- Recycle...

Edit Application Pool

- Basic Settings...
- Recycling...
- Advanced Settings...
- Rename

- (2) Click *Advanced Settings...*



Advanced Settings

(General)

- .NET Framework Version: v2.0
- Enable 32-Bit Applications: **True**
- Managed Pipeline Mode: True
- Name: False
- Queue Length: 1000
- Start Automatically: True

CPU

- Limit: 0
- Limit Action: NoAction
- Limit Interval (minutes): 5
- Processor Affinity Enabled: False
- Processor Affinity Mask: 4294967295

Process Model

- Identity: ApplicationPoolIdentity
- Idle Time-out (minutes): 20
- Load User Profile: False
- Maximum Worker Processes: 1
- Ping Enabled: True
- Ping Maximum Response Time (seconds): 90
- Ping Period (seconds): 30
- Shutdown Time Limit (seconds): 90
- Startup Time Limit (seconds): 90

Enable 32-Bit Applications

[enable32BitAppOnWin64] If set to true for an application pool on a 64-bit operating system, the worker process(es) serving the application pool will be in WOW64 (Windows on Windows64) mode. Processes in WOW64 mode are 32-bit processes...

OK Cancel

- (3) Change the *Enable 32-Bit Applications* setting to *True* and click *OK*.

Configuring a Proxy Trust List

The default XFF4IIS.ini file is located in the application installation directory at:

```
C:\Program Files\Winfrasoftware X-Forwarded-For for IIS\XFF4IIS.ini
```

The content of the default file is as follows:

```
[Config]
TrustList=

# Winfrasoftware X-Forwarded-For for IIS 2.0 configuraiton file usage
# -----
# Always Start the file with [Config] (Case sensitive)
# TrustList=xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy, zzz.zzz.zzz.zzz (Comma
# separated, valid IP addresses of trusted servers)

# Example:
# TrustList=192.168.0.100, 192.168.0.101, 192.168.0.200, 192.168.0.201
```

The file can be edited in notepad by double clicking it.

Simply list all the IP addresses of trusted proxy servers in your network through which traffic will flow through on route to the web server. Each IP address must be separated by a comma and a space and must only be on one line. Trusted proxy server IP addresses do not need to be in any particular order.

Only a valid IP address format will be accepted. Fully Qualified Domain Names and NetBIOS names will be ignored.

The details within the INI are case-sensitive and must conform to the layout specified in the sample above. Should X-Forwarded-For for IIS detect a non-conforming .INI file format, it will operate as if the configuration file is missing or no trust list exists.



Note

The IIS must be restarted in order for the Trust list changes to become active. It is recommended to run *IISRESET* at the command prompt.

Additional Information

“How to” guides

How to enable debug logging on X-Forwarded-For for IIS:

(<http://www.winfrasoft.com/kb-26.htm>)

Web Proxy Chaining as a Form of Network Routing:

(<http://www.isaserver.org/tutorials/Web-Proxy-Chaining-Form-Network-Routing.html>)

Support guides

X-Forwarded-For vulnerabilities in various platforms (Source: IBM ISS):

(<https://webapp.iss.net/Search.do?keyword=X-Forwarded-For&searchType=keywd>)

W3C Extended Log File Format (IIS 6.0):

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/676400bc-8969-4aa7-851a-9319490a9bbb.mspx?mfr=true>

For the latest information, see the Winfrasoft web site - <https://winfrasoft.com>.

Do you have comments about this document? Send feedback to feedback@winfrasoft.com