



Winfrasoft **XFF**
X-Forwarded-For for TMG

Installation and configuration guide

Adding X-Forwarded-For support to Forward and Reverse Proxy TMG Servers

Published: May 2010
Applies to: Winfrasoft X-Forwarded-For for TMG 2.1.1
Web site: <http://www.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
DESIGN AND DEPLOYMENT SCENARIOS	6
FORWARD PROXY WEB CHAINS – SCENARIO #1	6
FORWARD PROXY WEB CHAINS – SCENARIO #2	8
REVERSE PROXY WEB PUBLISHING – SCENARIO #1	10
X-FORWARDED-FOR AND SECURITY	11
BACKGROUND.....	11
ISA SERVER IMPLEMENTATION.....	11
WEB SERVER SECURITY.....	12
ALWAYS ON FORWARD PROXY CONFIGURATION	13
SSL TUNNEL CONFIGURATION FOR FORWARD PROXY.....	13
REMOVING INBOUND X-FORWARDED-FOR DATA	14
DEPLOYMENT	15
OVERVIEW	15
INSTALLING X-FORWARDED-FOR FOR TMG	16
<i>Automated installation</i>	18
UNINSTALLING X-FORWARDED-FOR FOR TMG.....	19
CONFIGURATION REVIEW	20
TMG ENTERPRISE EDITION	20
ADDITIONAL INFORMATION	21
“HOW TO” GUIDES	21
SUPPORT GUIDES.....	21

Introduction

X-Forwarded-For for TMG is a web filter application that integrates with both Standard and Enterprise Editions of TMG 2010 systems to:-

- Track the original IP address of a web client connecting to a web server through a forward or reverse proxy server.
- Track the original IP of SSL Tunnels through a forward proxy chain.
- Store the original client IP and intermediate proxy IP information in the X-Forwarded-For field of a HTTP request header.
- Maintain X-Forwarded-For header information through multiple proxy chains (no hard coded limit).
- Remove the X-Forwarded-For header information on the last forward proxy in the chain to prevent internal/private IP information being sent to the Internet. This behaviour can be configured.
- Remove inbound X-Forwarded-For header information from a proxy request.
- Log the original client IP as the Client IP address in ISA Server.
- Support both HTTP and HTTPS traffic for reverse proxy deployments. HTTPS functionality is reliant on a SSL certificate being installed on the ISA Server and bound to a web listener – X-Forwarded-For for TMG cannot be used with Server Publishing.
- Integrate with other 3rd party products that support the X-Forwarded-For de facto standard.

Considerations

Server System Requirements

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

- X64 systems with Windows Server 2008 R2
- Microsoft Forefront Threat Management Gateway
 - 2010 Standard Edition
 - 2010 Enterprise Edition

Language Requirements

Server

X-Forwarded-For for TMG is compatible with multi-lingual versions of Windows Server 2008 and TMG, however is only available in English. Product support and documentation is only available in English.

Licensing

X-Forwarded-For for TMG is licensed on a per server basis. A licence file must be installed onto each TMG Server (Standard Edition) or Array (Enterprise Edition) otherwise the application will function in trial mode.

To install the Winfrasoft X-Forwarded-For for TMG licence file simply run the supplied licence script file on the TMG Server which requires a licence. When using TMG Enterprise Edition, the licence script file need only be run on one TMG Server within the array, however no issues will arise if the licence file is run on more than one server.



Note

For detailed information on the licence types please refer to the licence agreement document embedded within the installation package.

Running a trial

When X-Forwarded-For for TMG 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 TMG will continue to function as though X-Forwarded-For for TMG was not installed.

If the *Microsoft Forefront TMG Firewall* service is restarted after 14 days then X-Forwarded-For for TMG will continue to function again for a further 2 hours. A TMG Alert and a Windows Event Log entry will be created to indicate this.

The screenshot displays the Microsoft Forefront TMG console interface. The main window shows the 'Alerts' tab with a table of recent alerts. The selected alert is 'X-Forwarded-For-Information'.

Alert	Latest	Status	Category	Server
Service Shutdown	1/14/2010 8:56:47 AM	New	Firewall Service	WIN-DJPC7JHU4C9
Network Inspection System Sign...	1/14/2010 8:57:44 AM	New	Firewall Service	WIN-DJPC7JHU4C9
Malware Inspection Definitions L...	1/14/2010 8:58:31 AM	New	Other	WIN-DJPC7JHU4C9
Service Started	1/14/2010 8:59:45 AM	New	Firewall Service	WIN-DJPC7JHU4C9
X-Forwarded-For-Information	1/14/2010 9:00:10 AM	New	Firewall Service	WIN-DJPC7JHU4C9
X-Forwarded-For-Information	1/14/2010 9:00:10 AM	New	Firewall Service	WIN-DJPC7JHU4C9

Below the table, the 'Alert Information' section shows the following description:

Description: The filter is running in demo/lab mode. It will run for 2 hours from the firewall start time.

An 'Event Properties' dialog box is overlaid on the console, showing details for 'Event 1, X_Forwarded_For Filter':

- Log Name: Application
- Source: X_Forwarded_For Filter
- Event ID: 1
- Level: Information
- User: N/A
- OpCode:
- More Information: [Event Log Online Help](#)
- Logged: 1/18/2010 7:45:04 AM
- Task Category: None
- Keywords: Classic
- Computer: WIN-DJPC7JHU4C9

Design and Deployment Scenarios

Winfrasoft X-Forwarded-For for TMG has been designed to fulfil the following security and logging scenarios. The product will function in many 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.

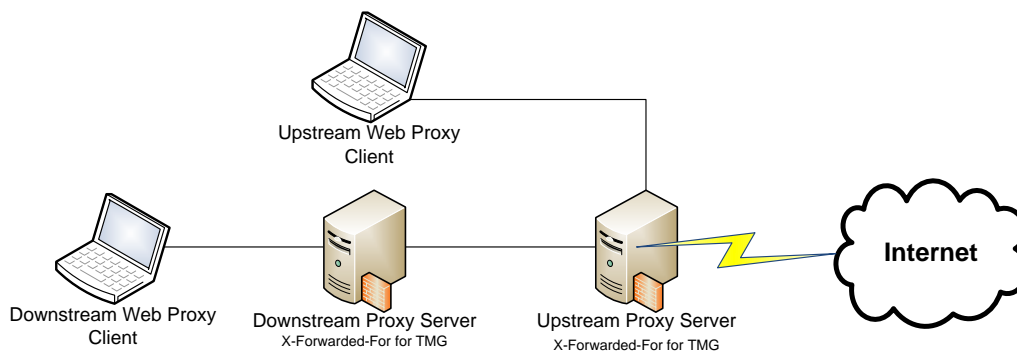


Note

The functionality of X-Forwarded-For for TMG is fixed and cannot be modified or customised other than being enabled or disabled through the TMG Management Console. There is no user interface for X-Forwarded-For for TMG.

Forward Proxy Web Chains – Scenario #1

This scenario describes the functionality of X-Forwarded-For for TMG in a forward proxy environment with one upstream and one downstream proxy configured in a web proxy chain. Behaviour of Web clients connecting to both the upstream and downstream proxy servers is detailed.

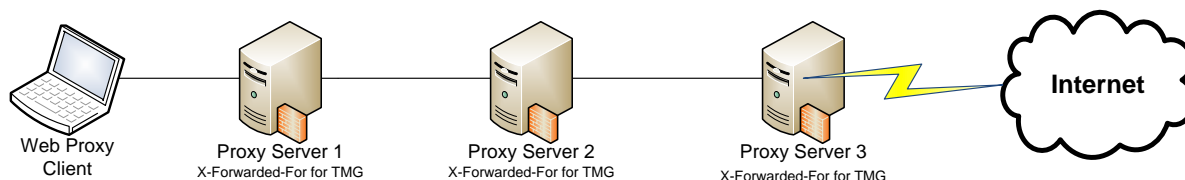


Proxy Server	
Downstream Proxy Server	<p>Add a "X-Forwarded-For" field containing the original client IP address to the HTTP header of a request when chaining to an Upstream Proxy server.</p> <p>Header syntax where xxx.xxx.xxx.xxx is the original client IP address:</p> <pre>X-Forwarded-For: xxx.xxx.xxx.xxx</pre>
Upstream Proxy Server "X-Forwarded-For" field exists in header of HTTP Request	<p>When a "X-Forwarded-For" field exists within a received HTTP request, log the original client IP address from the X-Forwarded-For field into the "Client IP" field of the TMG Server log.</p>
	<p>Append the Downstream TMG Proxy server's IP address into the "Filter Information"</p>

	<p>field of the TMG Server log, preserving any existing filter data.</p> <p>TMG Server log "Filter Information" field syntax where <code>yyy.yyy.yyy.yyy</code> is the downstream proxy server IP address:</p> <pre>X-Forwarded-For Proxy=yyy.yyy.yyy.yyy</pre>
	<p>By default, remove the "X-Forwarded-For" field from the HTTP request before sending the request to the Internet. This prevents disclosing internal private IP information to the Internet.</p>
<p>Upstream Proxy Server "X-Forwarded-For" field does not exist in header of HTTP Request</p>	<p>Log the details of the HTTP request as per normal TMG Server logs. No further action is required.</p>

Forward Proxy Web Chains – Scenario #2

This scenario describes the functionality of X-Forwarded-For for TMG in an environment with 3 proxy servers configured in a web proxy chain.



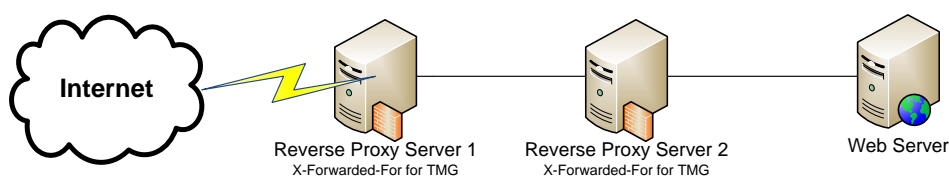
Proxy Server	
Proxy Server 1	<p>Add a “X-Forwarded-For” field containing the original client IP address to the HTTP header of a request when chaining to Proxy Server 2.</p> <p>Header syntax where xxx.xxx.xxx.xxx is the original client IP address: <code>X-Forwarded-For: xxx.xxx.xxx.xxx</code></p>
Proxy Server 2	<p>When a “X-Forwarded-For” field exists within a received HTTP request, log the original client IP address from the first X-Forwarded-For entry into the “Client IP” field of the TMG Server log. Note: At this stage there is only one X-Forwarded-For field entry.</p> <p>Append the IP address of Proxy Server 1 into the “Filter Information” field of the TMG Server log, preserving any existing filter data.</p> <p>TMG Server log “Filter Information” field syntax where yyy.yyy.yyy.yyy is the IP address of Proxy Server 1: <code>X-Forwarded-For Proxy=yyy.yyy.yyy.yyy</code></p>
	<p>Append the IP address of Proxy Server 1 to the “X-Forwarded-For” field, which already contains the original client IP address, to the HTTP header of a request when chaining to Proxy Server 3.</p> <p>Header syntax where xxx.xxx.xxx.xxx is the original client IP address and yyy.yyy.yyy.yyy is the IP address of Proxy Server 1: <code>X-Forwarded-For: xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy</code></p>
Proxy Server 3	<p>When a “X-Forwarded-For” field exists within a received HTTP request, log the original client IP address from the first X-Forwarded-For entry into the “Client IP” field of the TMG Server log.</p> <p>Append the IP address of Proxy Server 1 and 2 into the “Filter Information” field of the TMG Server log, preserving any existing filter data.</p> <p>ISA Server log “Filter Information” field syntax where yyy.yyy.yyy.yyy is the IP address of Proxy Server 1 and zzz.zzz.zzz.zzz is the IP address of Proxy Server 2:</p>

	<code>X-Forwarded-For Proxy=yyy.yyy.yyy.yyy, zzz.zzz.zzz.zzz</code>
	<p>By default, remove the “X-Forwarded-For” field from the HTTP request before sending the request to the Internet. This prevents disclosing internal private IP information to the Internet.</p> <p>This functionality can be disabled and the X-Forwarded-For header data can be retained for interrogation by transparent security gateways configured beyond the last of the web proxy servers.</p>

Reverse Proxy Web Publishing – Scenario #1

This scenario describes the functionality of X-Forwarded-For for TMG in an environment with 2 reverse proxy servers configured for web publishing. More than two reverse proxy servers can be used, or a mixture of TMG and other 3rd party devices that support the X-Forwarded-For header, e.g. some hardware load balancing devices.

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 will require a 3rd party plug-in, such as Winfrasoft X-Forwarded-For for IIS, to log the original client IP address on the Web Server using the X-Forwarded-For header information.



Proxy Server	
Reverse Proxy Server 1 “X-Forwarded-For” field does not exist in header of HTTP Request	<p>Add 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.</p> <p>Header syntax where xxx.xxx.xxx.xxx is the Internet original client IP address: <code>X-Forwarded-For: xxx.xxx.xxx.xxx</code></p>
Reverse Proxy Server 2	<p>When a “X-Forwarded-For” field exists within a received HTTP request, log the Internet original client IP address from the X-Forwarded-For field into the “Client IP” field of the TMG Server log.</p> <p>Append the IP address of Proxy Server 1 into the “Filter Information” field of the TMG Server log, preserving any existing filter data.</p> <p>TMG Server log “Filter Information” field syntax where yyy.yyy.yyy.yyy is the IP address of Proxy Server 1: <code>X-Forwarded-For Proxy=yyy.yyy.yyy.yyy</code></p>
	<p>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.</p> <p>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: <code>X-Forwarded-For: xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy</code></p>



Note

If Reverse Proxy Server 1 receives a request from the Internet that already contains an X-Forwarded-For header it shall retain the received data as per the behaviour of Reverse Proxy 2. See the X-Forwarded-For and Security section for further information on the implications of this.

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 TMG and 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.

ISA Server implementation

Although TMG will log the original client IP address as that specified in the X-Forwarded-For header, TMG will not apply firewall rules to that source IP address. TMG will still apply firewall rules based on the packet source IP address and not the X-Forwarded-For based original client IP address. As such TMG firewall rules cannot be subverted by spoofed X-Forwarded-For entries.

Outbound traffic

By default, Winfrasoft X-Forwarded-For for TMG protects internal IP information by removing the X-Forwarded-For field from the HTTP header when it detects that it is the last proxy server in a chain, i.e when there is no web chaining rule. As such, the proxy server closest to the Internet will remove the X-Forwarded-For data before the request is made to the Internet.

All X-Forwarded-For information in the chain is assumed to be trusted as it is made up of only internal IP addresses. The potential risk of an internal attack is still valid, however it is unlikely as little value could be gained from it. To help prevent internal attacks X-Forwarded-For information can be removed from the first inbound server in the chain.

X-Forwarded-For for TMG can also be configured to *not remove* the X-Forwarded-For header information if it is the last proxy in a chain. This configuration may be useful where a

transparent network device exists between the ISA Server and the Internet which needs to read/log the X-Forwarded-For header information. See the *Always On forward proxy configuration* section for further details.

Inbound 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. X-Forwarded-For for TMG does not utilise a proxy trust list thus this must be maintained on the web server – e.g. using Winfrasoft X-Forwarded-For for IIS on a web server. X-Forwarded-For for TMG however will verify that data received in the X-Forwarded-For header is valid data and an invalid or corrupt header will be removed.

X-Forwarded-For for TMG will always use the first X-Forwarded-For entry as the Client IP address when logging the traffic however the real IP packet header is processed by the TMG Firewall engine. If a X-Forwarded-For spoof is suspected, analyse the Filter Information field to verify the IP addresses of the listed X-Forwarded-For Proxy servers.

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

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.

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

Always On forward proxy configuration

X-Forwarded-For for TMG has the ability to always include the X-Forwarded-For header information regardless of Web Chaining rules. This is done by enabling the “SendToInternet” setting.

The X-Forwarded-For for TMG download includes a scripts folder which contains the following configuration script files:

- `SendToInternetOn.js`
- `SendToInternetOff.js`

These scripts configure the functionality of X-Forwarded-For for TMG installed on the last proxy server in a chain with regards to the retention of the X-Forwarded-For HTTP header data.

By default, the “SendToInternet” setting is set to OFF for security reasons – see the *X-Forwarded-For and Security* section for further information. Running the *SendToInternetOn.js* script enables the sending of the X-Forwarded-For header data to traffic routing to the Internet. This will allow any security gateways between the TMG Server and the Internet to interrogate the HTTP header data and retrieve the X-Forwarded-For information for the request. To disable this function simply run the *SendToInternetOff.js* script.



Warning

Exposing X-Forwarded-For information to the Internet is a potential security risk. Winfrasoft recommends that you enable this functionality only if another method exists to remove this information from HTTP packet headers before they reach the Internet.

SSL Tunnel configuration for forward proxy

X-Forwarded-For for TMG, by default, does not track Client IP information for SSL Tunnel traffic for a forward proxy. X-Forwarded-For header information is added to various HTTP requests, e.g. GET, POST etc. However, when SSL is used these request are all encrypted between the browser and the destination web server and are thus not visible to TMG or the X-Forwarded-For filter.

A SSL Tunnel is created through a web proxy server via a HTTP CONNECT request (<http://www.ietf.org/rfc/rfc2817.txt>). Within TMG these requests are not processed in the same way as usual HTTP traffic as TMG knows that the traffic is encrypted. As such, the inclusion of the X-Forwarded-For header information cannot be dynamically added based on Web Chaining rules. Adding X-Forwarded-For header information to track SSL Tunnels must be explicitly enabled for the server / array by enabling the “SendToInternetSSL” setting.

The X-Forwarded-For for TMG download includes a scripts folder which contains the following configuration script files:

- `SendToInternetSSLOn.js`
- `SendToInternetSSLOff.js`

The “SendToInternetSSL” setting is disabled by default for security reasons.

Removing Inbound X-Forwarded-For data

There may be scenarios, e.g. the first proxy server in a chain, where you want to ensure that no prior (e.g. spoofed) X-Forwarded-For data is added to your proxy chain list. To achieve this you need to configure the first server in the chain to drop any X-Forwarded-For data that may have been received before adding the client IP to the X-Forwarded-For header list.

To configure X-Forwarded-For for TMG to start with clean X-Forwarded-For header information the “IgnoreIncomingXFF” setting must be enabled by running the *IgnoreIncomingXFFOn.js* script.

The X-Forwarded-For for TMG download includes a scripts folder which contains the following configuration script files:

- *IgnoreIncomingXFFOn.js*
- *IgnoreIncomingXFFOff.js*

The “IgnoreIncomingXFF” setting is disabled by default to allow for normal proxy chain operation.

Deployment

Overview

This deployment section assumes that the Web Proxy chain has been established.

**Note**

This guide does not detail how to establish Upstream and Downstream Web proxy servers. See the Microsoft product documentation for assistance in deploying web proxy servers on TMG.

To fully deploy the X-Forwarded-For for TMG solution the following 4 steps must be performed:

- (1) Deploy and configure Web Proxy services and test functionality on TMG
- (2) Install X-Forwarded-For for TMG on the TMG Web Proxy Server
- (3) Ensure the X-Forwarded-For for TMG Web Filter is enabled
- (4) Check TMG logs and verify traffic using a network sniffer like Network Monitor. Also verify web server logs and behaviour when using TMG as a reverse proxy server.

Installing X-Forwarded-For for TMG

When X-Forwarded-For for TMG is first installed, the setup routine will, by default, create and enable the web filter on the TMG Server.



Note

The installation of the X-Forwarded-For for TMG may have problems with UAC during the install process. It is recommended to be logged onto the server with an account that has local administrator rights.

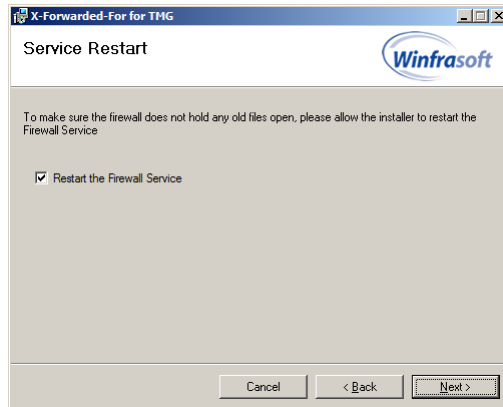
- (1) To start the X-Forwarded-For for TMG installation run the *XFFforTMG2.1.0.msi* installation package using *Administrator Privileges*.
- (2) This starts the setup wizard:



- (3) Click *Next* to continue.

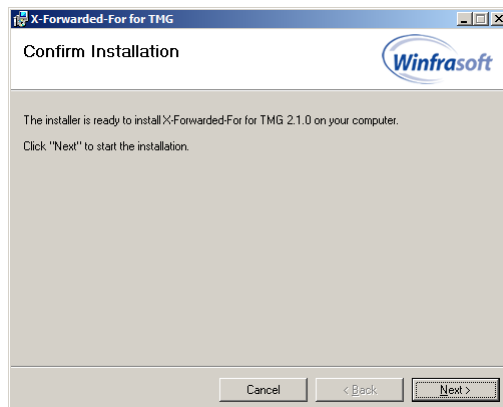


- (4) After reading the licence agreement click *I Agree* if you agree to the terms, then click *Next* to continue.

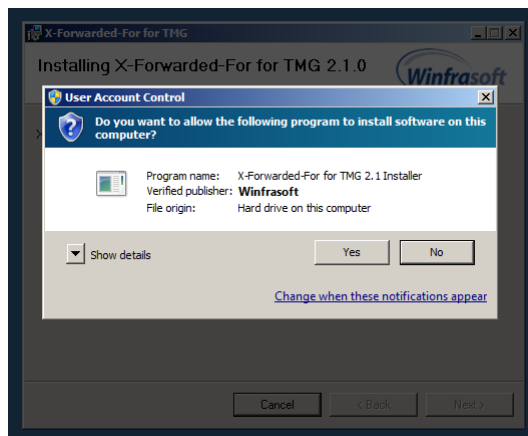
**Note**

Installation of the X-Forwarded-For for TMG web filter requires a restart of the Microsoft Forefront TMG Firewall service. It is recommended to check the *Restart the Firewall Service* box during installation.

- (5) Click *Next* to continue.

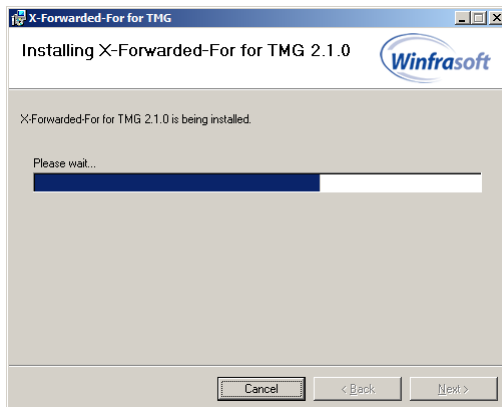


- (6) Click *Next* to continue.

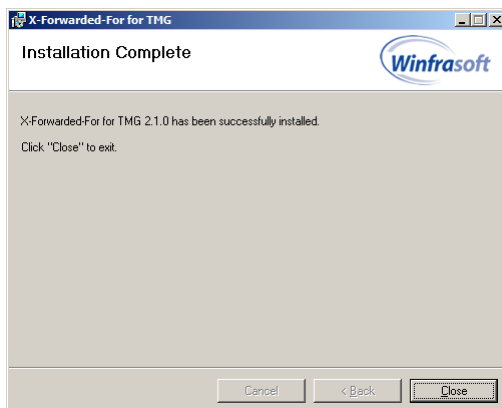


18 Winfrasoft X-Forwarded-For for TMG 2.1

- (7) If prompted by UAC ensure the **Program name** and **Verified publisher** are correct and click *Yes* to allow the installation.



The installation is performed and the services restarted.



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

Automated installation

The X-Forwarded-For for TMG installation can be automated on TMG 2010 by running the following from an **administrator elevated** command prompt:

```
msiexec /passive /i XFFforTMG2.1.0.msi
```

Should the automated install require additional CSS and domain credentials, utilise the following command:

```
msiexec /passive /i XFFforTMG2.1.0.msi CSSSERVER=<ipaddress/dnsname>  
CSSDOMAIN=<domainname> CSSUSER=<username> CSSPASSWORD=<password>
```



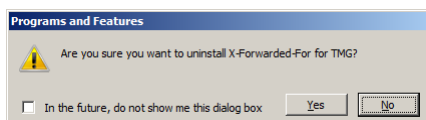
Note

The Microsoft Forefront TMG Firewall service will be automatically restarted during an automated installation.

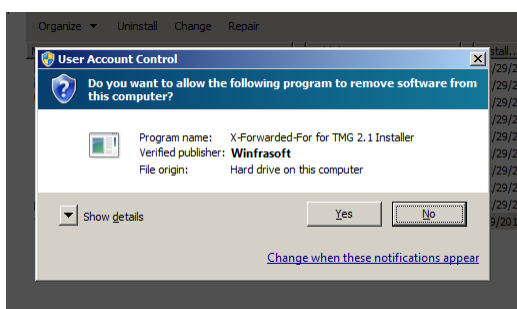
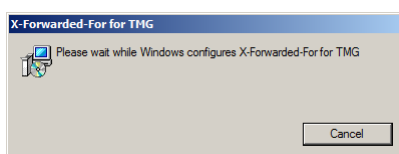
Uninstalling X-Forwarded-For for TMG

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

- (1) To start the X-Forwarded-For for TMG automated un-installation use Add/Remove Programs in the Control Panel and click Remove.



- (2) Click *Yes* to begin the removal.

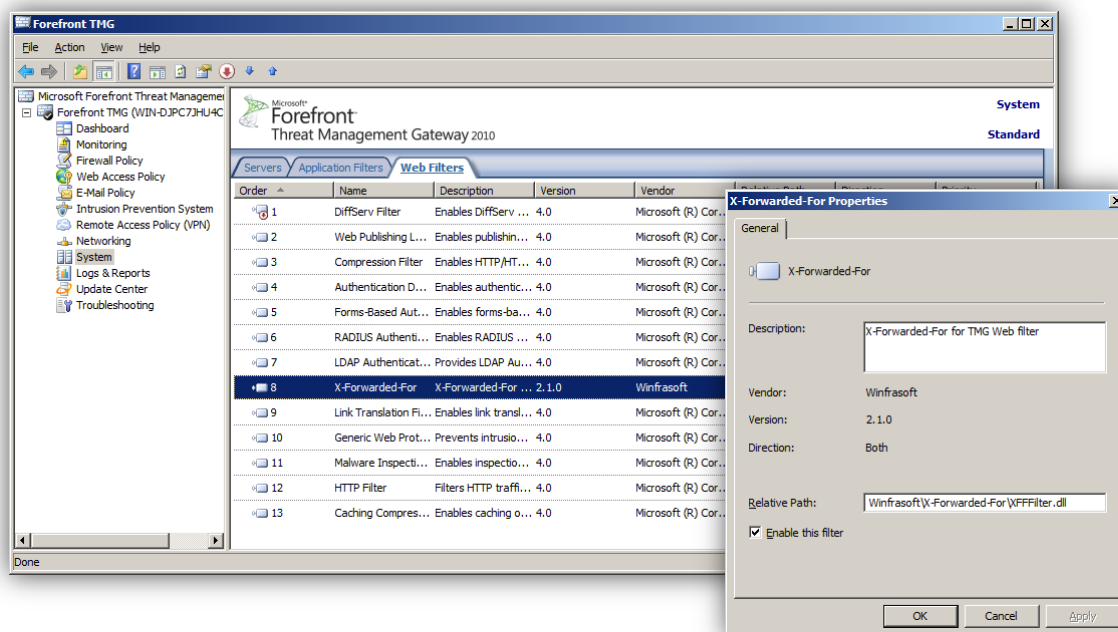


- (3) If prompted by UAC ensure the **Program name** and **Verified publisher** are correct and click *Yes* to allow the removal.

This will automatically restart the Microsoft Forefront TMG Firewall Service without prompting.

Configuration review

After the installation of X-Forwarded-For for TMG, the filter will automatically appear in the Web Filters tab of System section in the TMG Management console as follows:



Note

X-Forwarded-For for TMG can be enabled/disabled and moved up and down in the priority list through the TMG Management console.

TMG Enterprise Edition

X-Forwarded-For for TMG is designed to work with TMG Enterprise Edition and must be installed on all servers in an array. However, the licence only needs to be installed on a single node as this data is stored in the CSS / EMS configuration and will automatically apply to all array members.

X-Forwarded-For for TMG is CARP aware. As such, if traffic is routed from a web proxy client to the incorrect array member, the X-Forwarded-For header will be appended within the array communication so that the original client IP is still retained. Traffic originating with the array, i.e. Intra Array Communication traffic will not have X-Forwarded-For header information applied as it is not required.

Additional Information

“How to” guides

Forefront TMG Deployment

(<http://technet.microsoft.com/en-us/library/cc441445.aspx>)

Chaining Concepts in ISA Server 2006:

(<http://www.microsoft.com/technet/isa/2006/chaining.mspx>)

Web Proxy Chaining as a Form of Network Routing:

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

Publishing Concepts in ISA Server 2006:

(http://www.microsoft.com/technet/isa/2006/deployment/publishing_concepts.mspx)

Support guides

Microsoft ISA Server 2006 – Operations:

(<http://www.microsoft.com/technet/isa/2006/operations/default.mspx>)

Troubleshooting Web Proxy Traffic in ISA Server 2004:

(http://www.microsoft.com/technet/isa/2004/plan/ts_proxy_traffic.mspx)

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

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

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

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