Winfrasoft

Installation and Configuration

Guide

Installation and configuration guide

Adding X-Username support to Forward and Reverse Proxy TMG Servers

Published: December 2010

Applies to: Winfrasoft X-Username for TMG 1.0.0.1

Web site: http://www.winfrasoft.com

Email: support@winfrasoft.com

Microsoft GOLD CERTIFIED Partner

Security Solutions
ISV/Software Solutions
Networking Infrastructure Solutions

Table of Contents

Introduction

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

- Track the original username of a web client connecting to a web server through a forward or reverse proxy server in the HTTP request header.
- Supports original username tracking when proxy to proxy authentication is utilised.
- Maintain X-Username header information through multiple proxy chains.
- Remove the X-Username header information on the last forward proxy in the chain to prevent internal/private information being sent to the Internet. This behaviour can be configured.
- Log the original client username on TMG server.
- Support both HTTP and HTTPS traffic for forward and reverse proxy deployments. HTTPS functionality is reliant on a SSL certificate being installed on the TMG Server and bound to a web listener – X-Username for TMG cannot be used with Server Publishing.

Considerations

Server System Requirements

The minimum system requirements for X-Username for TMG are:

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

Language Requirements

Server

X-Username 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-Username 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.

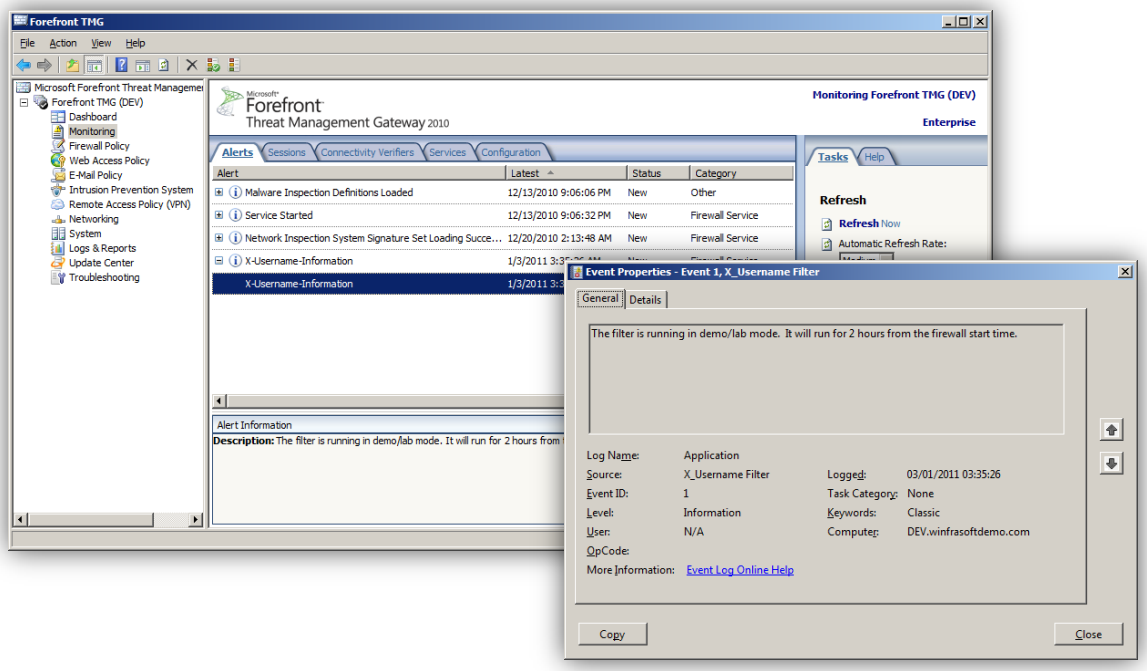
To install the Winfrasoft X-Username for TMG licence file simply run the supplied licence script file on the TMG Server which requires a licence. When using TMG Enterprise Edition, the licence script file need only be run on one TMG Server within the array, however no issues will arise if the licence 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-Username 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-Username for TMG was not installed.

If the *Microsoft Forefront TMG Firewall* service is restarted after 14 days then X-Username 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.



Design and Deployment Scenarios

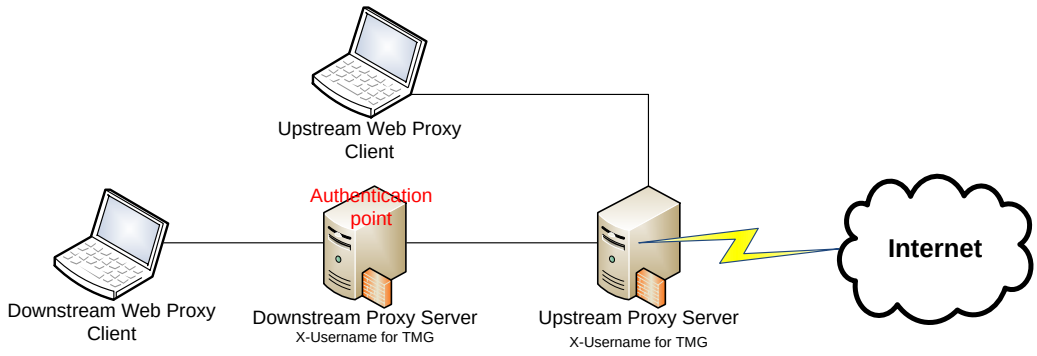
Winfrasoft X-Username for TMG has been designed to fulfil the following security and logging scenarios. The product will function with other TMG web filters, e.g. Winfrasoft X-Forwarded-For for TMG, however Winfrasoft is unable to test every combination, especially with 3rd party products. It is recommended that all deployment scenarios are tested in a lab prior to a live deployment.

Note

The functionality of X-Username for TMG can be modified via the included scripts and can be enabled or disabled through the TMG Management Console. There is no user interface for X-Username for TMG.

Forward Proxy Web Chains – Scenario #1

This scenario describes the functionality of X-Username 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.



Note

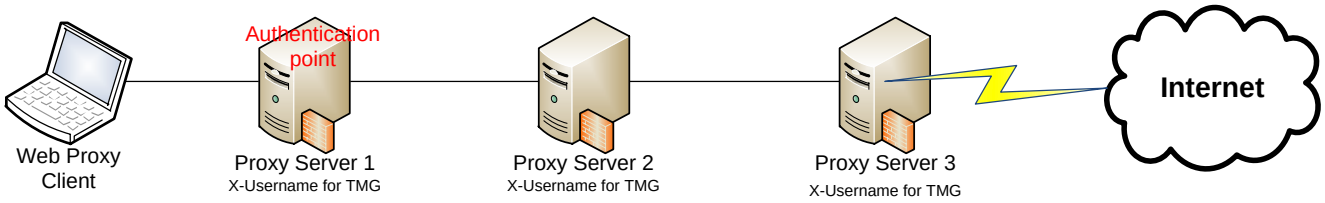
Spoofing of usernames can be prevented by establishing proxy to proxy authentication.

Proxy Server	
Downstream Proxy Server	Creates the HTTP header and adds the "X-Username" field containing the original client username to the HTTP header of a request when chaining to Upstream Proxy Server. Header syntax where domain\username is the original client username: `X-Username: domain\username`

Upstream Proxy Server “X-Username“ field exists in header of HTTP Request	When a “X-Username” field exists within a received HTTP request, log the original client username from the X-Username field into the “Client Username” field of the TMG Server log. `X-Username added 'domain\username' was ('anonymous')`
	By default, remove the “X-Username” field from the HTTP request before sending the request to the Internet if there is no further web chaining rule in place. This prevents disclosing internal private username information to the Internet. This functionality can be disabled and the X-Username header data can be retained for interrogation by transparent security gateways configured beyond the last of the web proxy servers.
Upstream Proxy Server “X-Username“ field does not exist in header of HTTP Request	Log the details of the HTTP request as per normal TMG Server logs. No further action is required.

Forward Proxy Web Chains – Scenario #2

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



Note

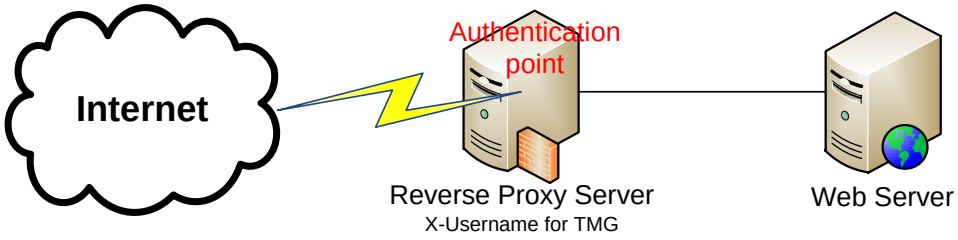
In the above scenario, X-Username must be installed on the first Proxy server in the proxy chain (Proxy Server1), and then on each Proxy server where you wish to log the X-Username information in the proxy logs.

Proxy Server	
Proxy Server 1	Creates the HTTP header and adds the "X-Username" field containing the original client username to the HTTP header of a request when chaining to Upstream Proxy Server. Header syntax where domain\username is the original client username: `X-Username: domain\username`
Proxy Server 2	When a "X-Username" field exists within a received HTTP request, log the original client username from the X-Username entry into the "Client Username" field of the TMG Server log.
	The web filter then determines that another proxy server exists in the proxy chain (Proxy Server 3) so the X-Username information will NOT be removed before forwarding the request.
	If the X-Username for TMG filter was not installed or disabled on Proxy Server 2 then the X-Username value will not be processed however it will be forwarded to the next server. It is typical behaviour of web proxy servers to forward on header information.
Proxy Server 3	When a "X-Username" field exists within a received HTTP request, log the original client username from the X-Username entry into the "Client Username" field of the TMG Server log.
	By default, remove the "X-Username" field from the HTTP request before sending the request to the Internet as it is the last proxy in the chain. This functionality can be disabled and the X-Username header data can be retained for interrogation by transparent security gateways configured beyond the last of the web proxy servers. This can be done by running the `SendToInternetOn.js` script on Proxy Server 3.

Reverse Proxy Web Publishing – Scenario

This scenario describes the functionality of X-Username for TMG in an environment with a reverse proxy server configured for web publishing.

The Web Server is responsible for processing the X-Username header information that is received. Microsoft IIS does not support X-Username natively and will require a 3rd party plug-in, such as Winfrasoft X-Username for IIS, to log the original client username on the Web Server using the X-Username header information.



Proxy Server	
Reverse Proxy Server "X-Username" field does not exist in header of HTTP Request	Add the "X-Username" field containing the original client username to the HTTP header of a request when Web Publishing to the web server. Header syntax where domain\username is the original client username: `X-Username: domain\username`
Web Server	When a "X-Username" field exists within a received HTTP request the web server should respond according. This may simply be to log the client username in the web server log or it may feed it into the functionality of a web application. The functionality is dependent on the web server.

Note

See the Winfrasoft X-Username for IIS documentation for further information about adding X-Username capabilities to IIS.

X-Username and Security

Background

Historically, in both Microsoft ISA Server 2004/2006 and Microsoft Forefront TMG 2010, there has been no method in which to track the client username through a forward proxy chain. It is possible to track a username through a reverse proxy chain using delegation, however each proxy server must authenticate the given credentials which may lead to

performance or connectivity issues. To resolve these issues, Winfrasoft created a new HTTP header called X-Username.

X-Username 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-Username header especially if the data originates from the Internet.

Please be aware of the deployment nuances as a misconfiguration could result in sensitive internal infrastructure information being unwittingly divulged to the Internet.

There is no RFC or official standard for X-Username and as such vendors implement their own version of X-Username in their products which can lead to some incompatibilities. Different vendors may implement X-Username in different ways, as such, Winfrasoft cannot guarantee interoperability with other vendors.

TMG Server implementation

Although TMG will log the original client username as that specified in the X-Username header, TMG will not apply firewall rules to that username. As such TMG firewall rules cannot be subverted by spoofed X-Username entries.

Outbound traffic

By default, Winfrasoft X-Username for TMG protects internal user information by removing the X-Username 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-Username data before the request is made to the Internet.

All X-Username information in the chain is assumed to be trusted as it is made up of only internal user information. The potential risk of an internal attack is still valid, however it is unlikely as little value could be gained from it. To prevent X-Username spoofing attacks, it is recommended that one implements Proxy to Proxy authentication within a proxy server chain by specifying a connection account on the web chaining rule. By default, the proxy connection account will be ignored for the purposes of the X-Username processing, and the username in the received X-Username header will be used.

X-Username for TMG can also be configured to *not remove* the X-Username header information if it is the last proxy in a chain. This configuration may be useful where a transparent network device exists between the TMG Server and the Internet which needs be read/log the X-Username header information. See the *Always On forward proxy configuration* section for further details.

Inbound Traffic

It is critical to understand that using X-Username for inbound traffic is not a security substitution for authentication delegation, however it can be a very flexible option for logging purposes where further layers of authentication are not required.

The X-Username value is not signed or authenticated and should only be relied on (with care and caution) if the network topology between the reverse proxy and the web server is secure and not susceptible to injection attacks.

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

X-Username and SSL

X-Username for TMG is fully SSL aware and can track username information for SSL Tunnel traffic for forward and reverse proxy connections. X-Username 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-Username 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.

In a forward proxy scenario, the X-Username header is added to the HTTP CONNECT header, not within the SSL tunnel. This allows proxy servers to log the username even though the SSL traffic remains encrypted.

In a reverse proxy scenario there is no HTTP CONNECT request, as such the X-Username header is maintained within the encrypted tunnel, thus any proxy server which requires access to the X-Username data MUST be able to decrypt the SSL traffic, aka bridging.

X-Username vs. Authentication Conflicts

When a proxy server receives an anonymous request containing a X-Username header the expected behaviour is fairly simple. In this case the username value stored in the X-Username field is used in place of anonymous otherwise there would be no need for the filter to be installed.

However, there are scenarios where a proxy server could receive a request containing an X-Username header which is also authenticated. In this case the filters behaviour can be configured via the *ForwardIncoming* setting

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

- `ForwardIncomingOn.js`
- `ForwardIncomingOff.js`

By default, the ForwardIncoming setting is set to ON to mimic the behaviour of the proxy server prior to installing the filter. In this configuration the X-Username value which is received is always the value used when forwarding the request, regardless of whether the request was authenticated or not. This is useful when proxy to proxy authentication is used with a connection account and the original username must be retained. If no X-Username header is received on an authenticated connection then the username used for authentication is added to the X-Username field when the request is forwarded.

Running the *ForwardIncomingOff.js* script changes the default behaviour so that the user account name used during authentication is always used as a priority over the received value in the X-Username header. To restore the default functionality simply run the *ForwardIncomingOn.js* script.

Always On forward proxy configuration

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

The X-Username 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-Username for TMG installed on the last proxy server in a chain with regards to the retention of the X-Username HTTP header data.

By default, the SendToInternet setting is set to OFF for security reasons – see the *X-Username and Security* section for further information. Running the *SendToInternetOn.js* script enables the sending of the X-Username 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-Username information for the request. To disable this function simply run the *SendToInternetOff.js* script.

Warning

Exposing X-Username 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.

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-Username for TMG solution the following 4 steps must be performed:

(1) Deploy and configure Web Proxy services and test functionality of TMG

(2) Install X-Username for TMG on the TMG Web Proxy Servers

(3) Ensure the X-Username 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-Username for TMG

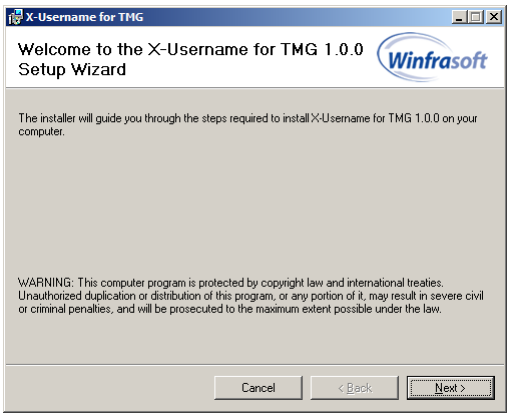
When X-Username for TMG is first installed, the setup routine will, by default, create and enable the web filter on the TMG Server.

Note

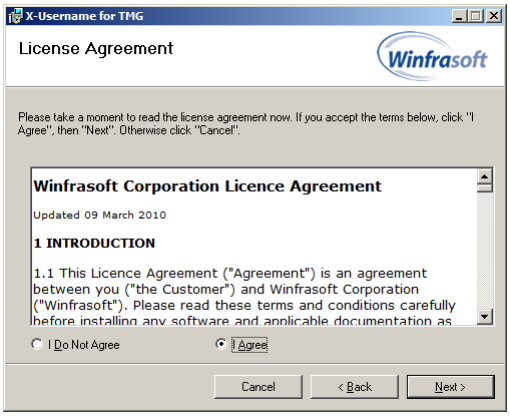
The installation of the X-Username for TMG may have problems with UAC during the install process. It is recommended to be logged onto the server with an account that has local administrator rights.

(1) To start the X-Username for TMG installation run the *XUNforTMG1.0.0.msi* installation package using *Administrator Privileges*.

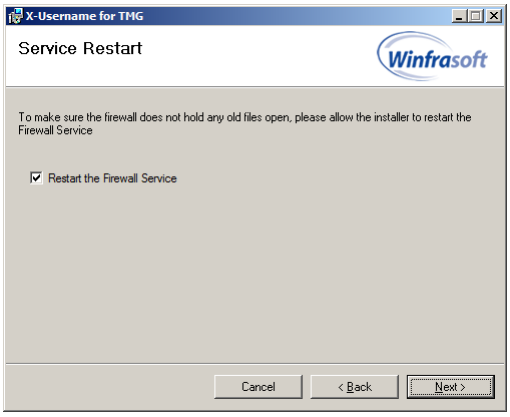
(2) This starts the setup wizard:



(3) Click *Next* to continue.



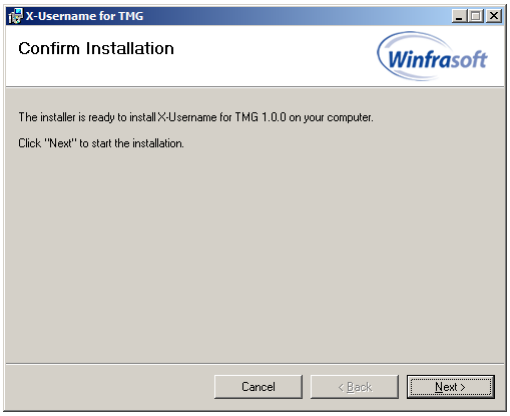
(4) After reading the licence agreement click *I Agree* if you agree to the terms, then click *Next* to continue.



Note

Installation of the X-Username 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.

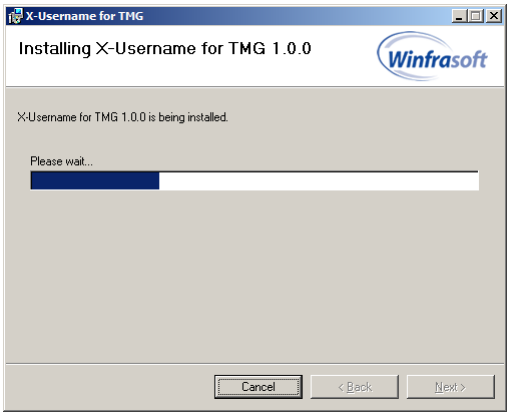
(5) Click *Next* to continue.



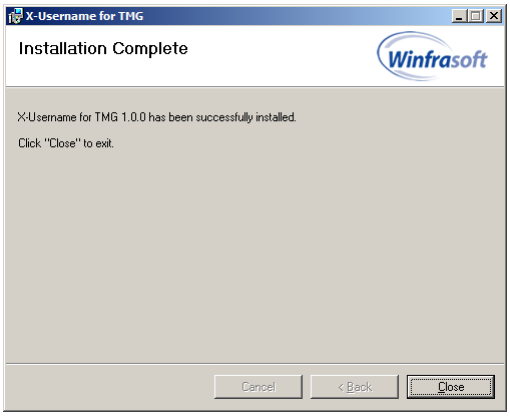
(6) Click *Next* to continue.

Note

You may be prompted by UAC to confirm the application installation. If prompted by UAC click Yes to allow the installation.



The installation is performed and the services restarted.



(7) Click *Close* to complete the installation process.

Automated installation

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

```
msiexec /passive /i XUNforTMG1.0.0.msi
```

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

```
msiexec /passive /i XUNforTMG1.0.0.msi CSSSEREVER=<ipaddress/dnsname>
CSSDOMAIN=<domainname> CSSUSER=<username> CSSPASSWORD=<password>
```

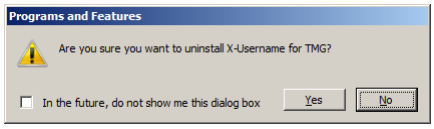
Note

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

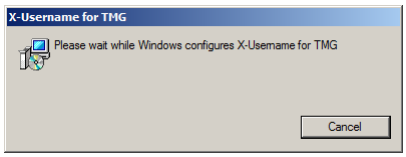
Uninstalling X-Username for TMG

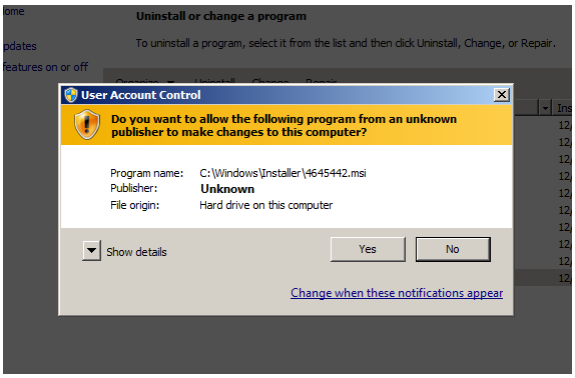
If you no longer require X-Username for TMG to be installed you and remove it from a server as follows:

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

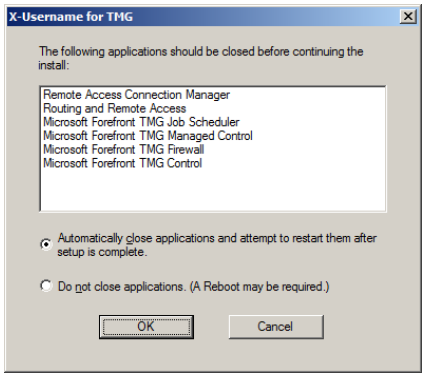


(2) Click *Yes* to begin the removal.





(3) If prompted by UAC click *Yes* to allow the removal.

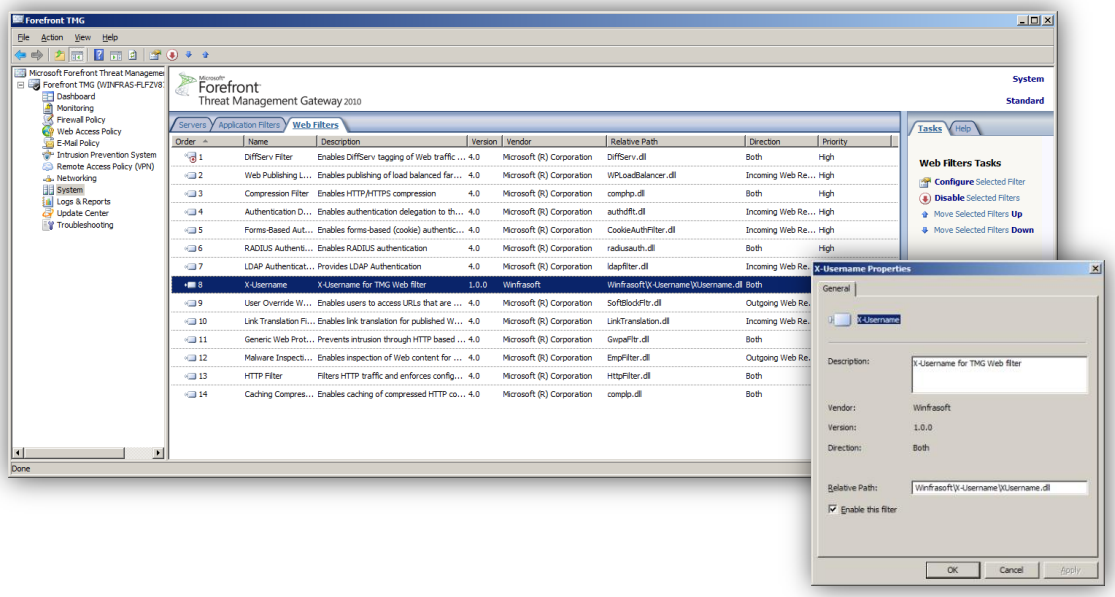


(4) To uninstall the web filter, certain application must be closed and restarted. Select *Automatically close applications and attempt to restart them after setup is complete.* Click *OK* to allow the removal.

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

Configuration review

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



Note

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

TMG Enterprise Edition

X-Username 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.

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

Forefront TMG Operations:

(http://technet.microsoft.com/en-gb/library/cc441590.aspx)

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)

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