
# WebTOS “Getting Started” User Guide

(The following graphics are screen shots from Microsoft® ISA Server 2004 which is the property of Microsoft Corp. and are included here for instructive use. Some images illustrate WebTOS, which is the property of Collective Software.)

## Table of Contents

## Problem Statement

- Your organization wants to display a “Terms of Service” screen or other preliminary page to internal users prior to letting them access the web.
- Your organization wants to display a TOS screen to outside Internet users before they are allowed access to one or more of your published HTTP/HTTPS servers.

## Solution Overview

Collective Software WebTOS was designed to seamlessly provide a customizable TOS screen to fit the above situations. WebTOS provides the following features:

- One customizable TOS screen for the Internal network.
- A second customizable TOS screen to present in front of your Internet HTTP and HTTPS published servers.
- Completely configurable settings per web listener; only enable WebTOS where you want it.
- Transparent integration with existing authentication systems; TOS is displayed before logon prompt for published servers.
- Configurable exemptions which prevent the TOS being shown when requests match certain values for any of the following:
    - Browser type (some HTTP clients cannot properly navigate a TOS)
    - IP address (don't show TOS on certain trusted machines)
    - URLs (useful for always-allow sites such as Windows Update)

WebTOS has a few limitations that should be noted as well:

- On the internal network, only HTTP traffic is subject to TOS; HTTPS and other protocols will not be presented with a TOS prompt or limited in any other way. For a more powerful quarantining solution, ask us about our WebQuarantine system.
- All externally published servers will be presented with the same TOS screen. Customizations per-server are still possible via clever use of client-side scripting technology, but by default this level of sophistication is not provided in the example TOS pages.
- For compatibility, all HTTP requests other than “GET” are permitted to pass without TOS. In practice this is not a concern, since in order to use “POST” or other methods, browsers must “GET” one or more pages first.
- If clients on the Inside network do not use SecureNAT, are not configured as Proxy clients, and do not use the Firewall Client, then their web

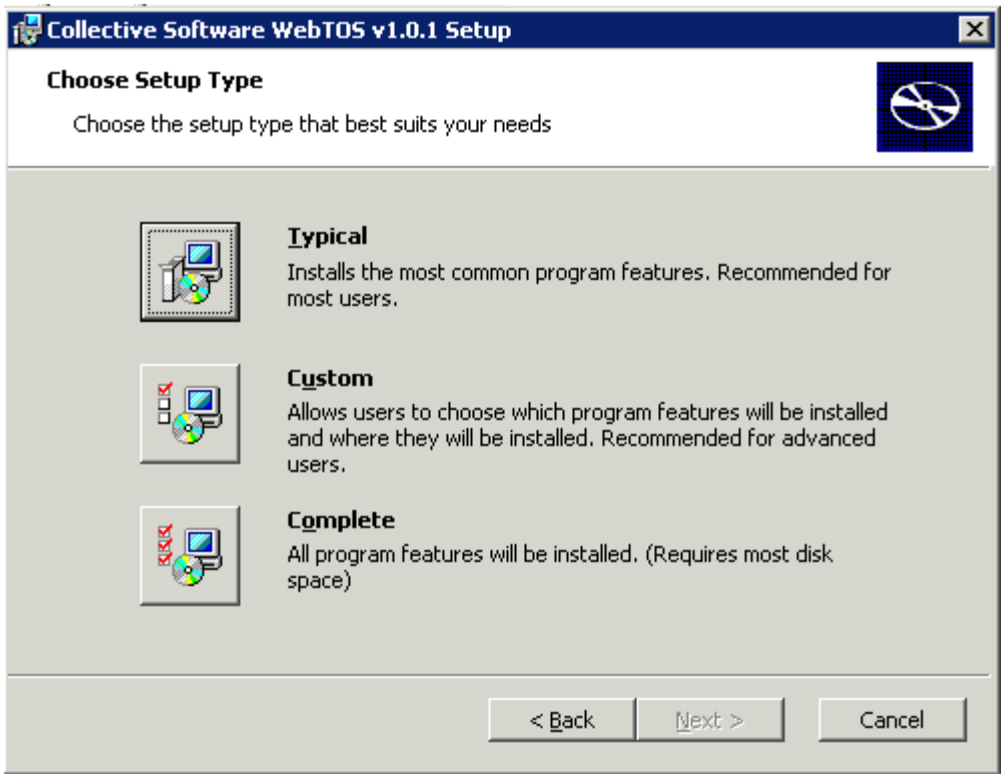
requests will not reach the ISA server. Therefore, in this scenario, WebTOS cannot be applied.

In the following sections, we will walk through the installation and configuration of WebTOS.

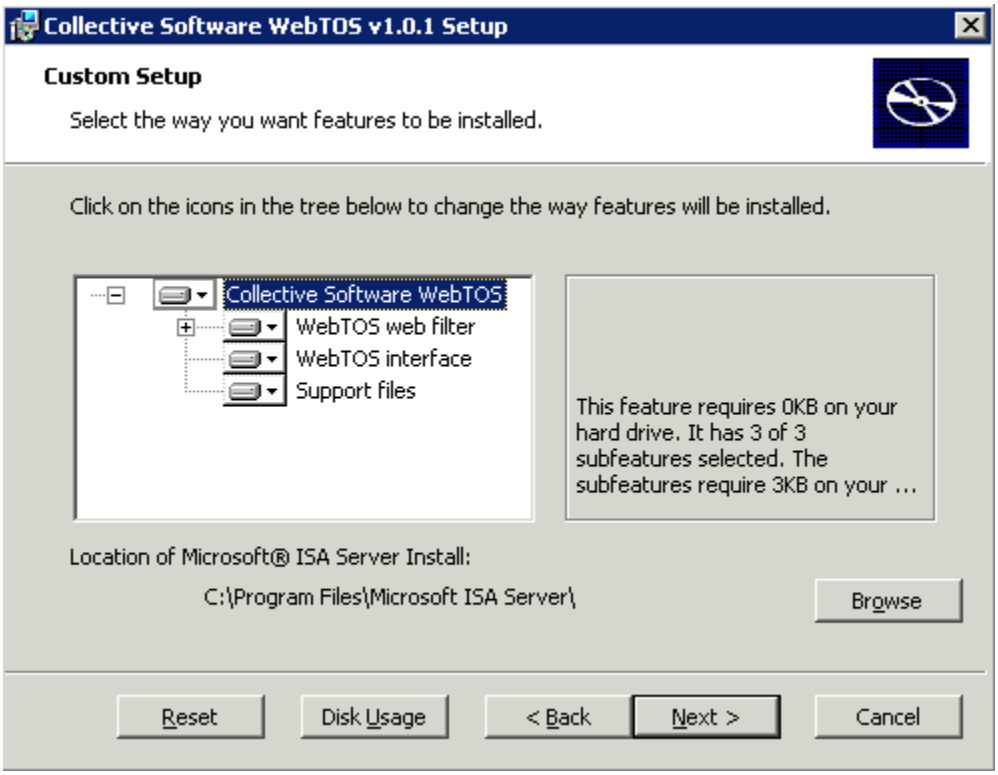
## Help is available!

We are always happy to help you get our software set up and working. If you have questions or need assistance understanding/configuring/testing a Collective product, you can get in touch with our support staff quickly and easily. For the most up-to-date information, please see our Support page at http://www.collectivesoftware.com/Support/

## Installation




The WebTOS installer's "Typical" settings assume that your ISA installation is in the default location (C:\Program Files\Microsoft ISA Server) and that you wish to install both the Web Filter and the User Interface components on the server. **You can change any of these items by selecting the "Custom" install mode:**




You *must* install at least the "WebTOS web filter" component on the ISA server itself. If you are using Enterprise Edition, this installer must be run separately on each of the ISA servers in your array.

You should install the "WebTOS interface" on all machines from which you will administer your ISA enterprise. This component extends the ISA console's "Web Listener" properties dialog and allows you to configure the WebTOS filter's functionality.

In the event of install difficulties, the Windows Event Log (Application section) will usually contain more information about the problem, and should be sufficient to resolve the issue in most cases.

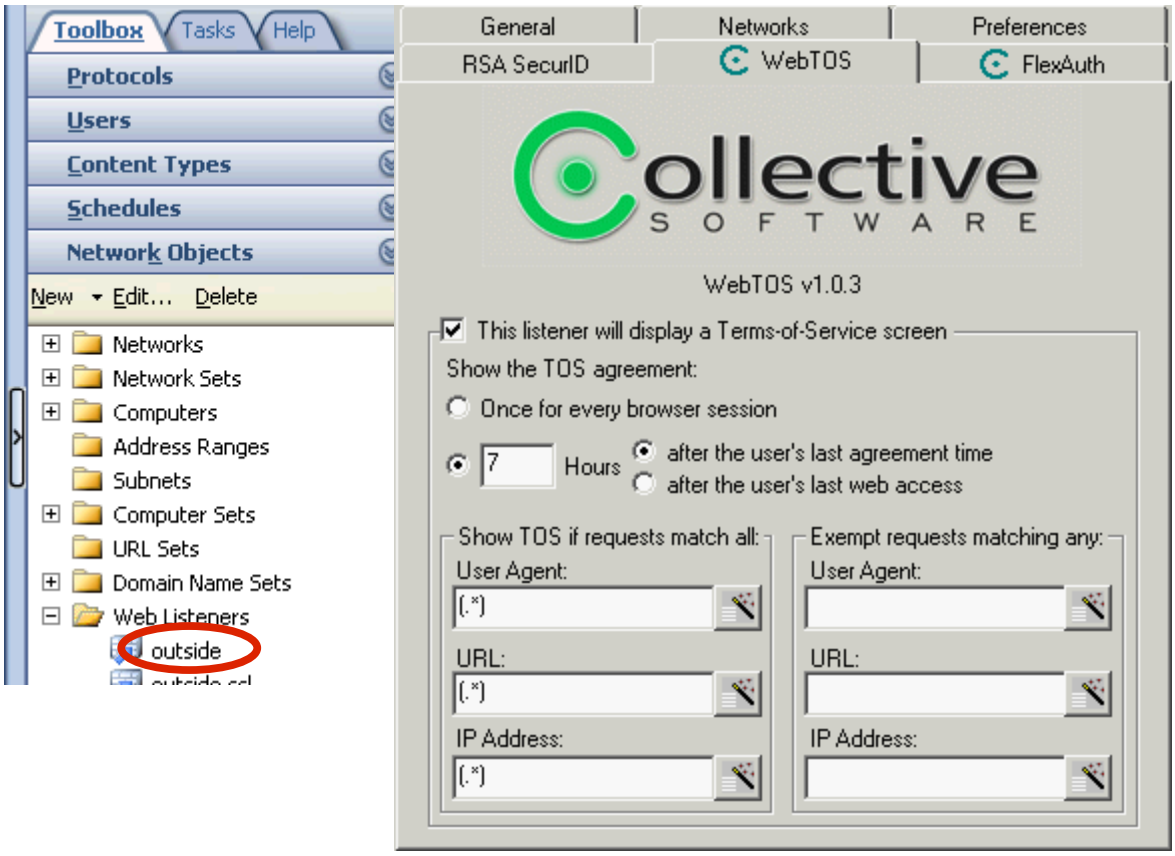
After installation, it is prudent to restart the Microsoft Firewall service to ensure the filter gets loaded properly.

NOTE: In most cases the installation will complete without requiring a restart. If a restart is needed, the Windows Installer should automatically let you know.

# Configuring WebTOS

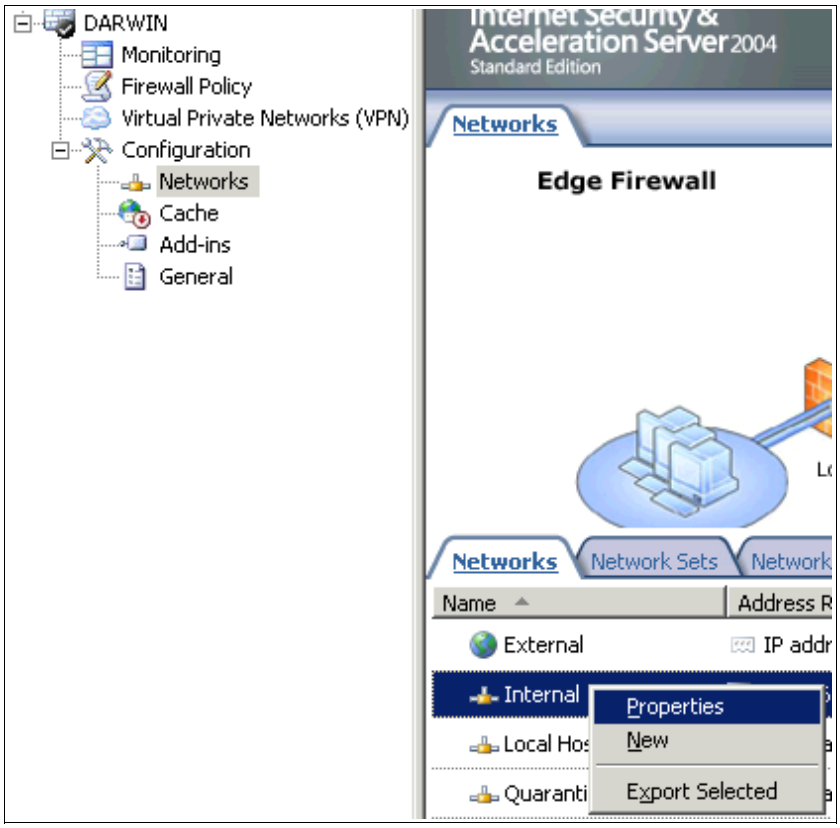
### *Accessing WebTOS properties for your published servers*

WebTOS adds a tab to the Web Listener properties dialog, which can be accessed from the Toolbox as shown here.



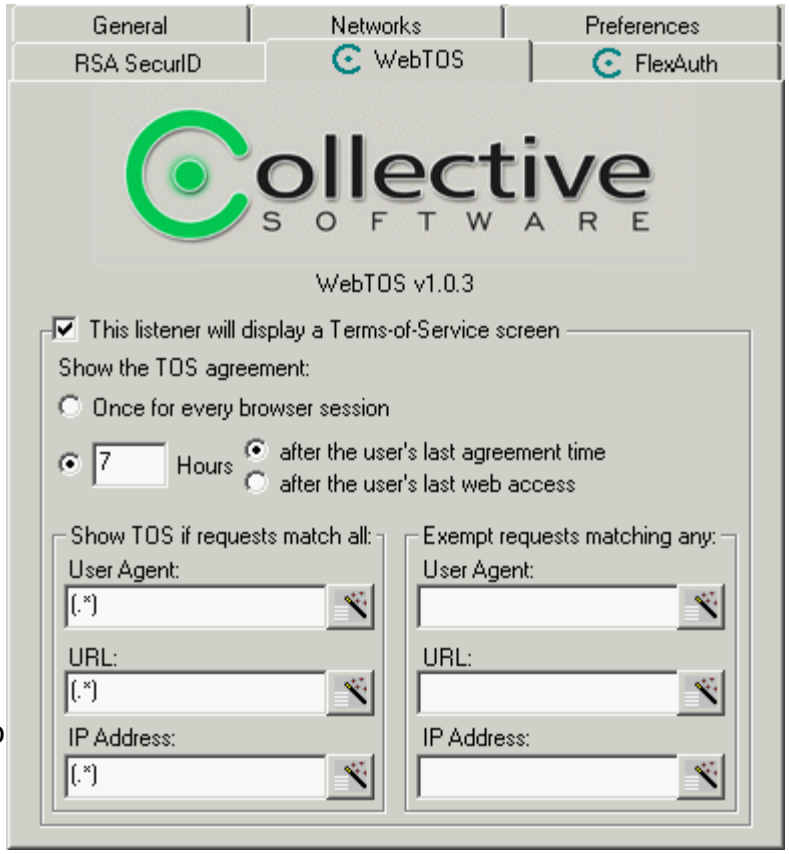

Please note that due to a limitation of the ISA console, accessing the Listener properties from the Publishing Rule properties dialog will *not* show the WebTOS tab. The WebTOS tab is only accessible in the manner shown above.

### *Accessing WebTOS properties for the Internal network*




The WebTOS properties for your Internal proxy users can be displayed by selecting “Properties” on the Internal network object.

***The WebTOS tab***




## Enabling

To enable TOS on a listener, check the main box on this tab.

## Display

For publishing listeners you have the ability to require a TOS agreement once per browser session. This option is **not** available for clients on the inside network who are proxying through ISA, due to technical limitations.

Instead of once per session, you can configure a certain number of hours between TOS displays. You can use either of two metrics for the timer:

- How long since the user has last seen a TOS and agreed to it
- How long since the user has last performed an HTTP request to this listener.

## Matching requests

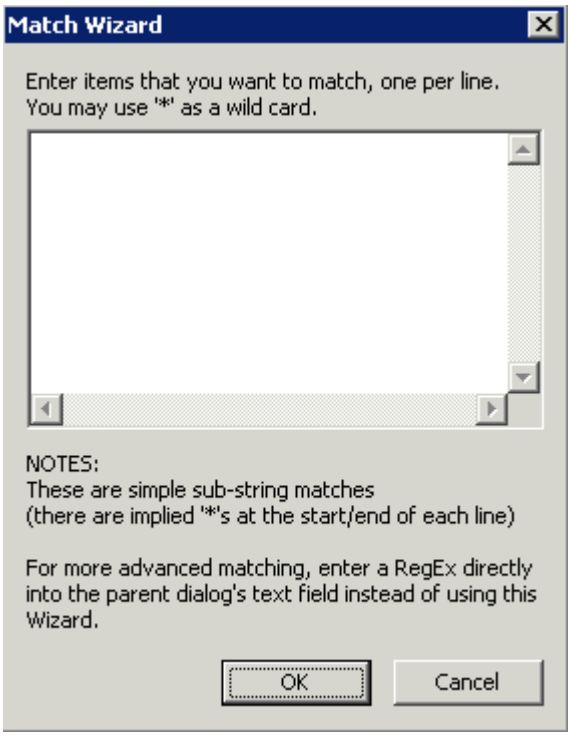
You may wish to limit certain types of requests from showing the TOS screen. By default if you change none of the match settings, all requests will be subject to TOS.

For each listener, there are six fields that control whether a web request will display a TOS screen.

- **Required match fields**:
  A request must match **all** of these fields in order for a TOS to be shown.
- **Exemption fields**:
  If a request does **not** match **any one** of these fields, the TOS will be suppressed.

These fields are Regular Expressions, however you don't have to be familiar with RegEx to use WebTOS. You can click the Match Wizard button and you will be

presented with the following dialog:




You can enter one match item per line and use the asterisk "*" character as a wild card. When you click "OK" the Wizard will convert your list of entries into the appropriate RegEx syntax. For more advanced matching, you can directly input RegEx syntax into the main dialog.

The three field types will be explained next:

- **User Agent**: Certain mobile browsers or other specialized clients may not function properly if presented with a TOS. You can use the user agent fields to match part of the "User-Agent" header. A simple configuration might be to match "MSIE" so that all Internet Explorer sessions are subject to TOS, but things such as ActiveSync can pass uninhibited. If you find there are some browsers (such as Palm devices) that contain "MSIE" in their user agent string, you could put "Palm" into the User Agent Exemption list. This configuration effectively means "Show TOS for all browsers that have 'MSIE' in the agent string but not if they also contain 'Palm' ".
- **IP Address**: In case you need to control TOS display per client IP address. Please note that these are **not IP/subnet matching fields**. So if you were to type "192.168.1.0/8" into the wizard it would **not** do what you want. Instead you could type "192.168.1.*" into the wizard.
- **URL**: Some services (such as Windows Update) can occur automatically without the user actually opening a browser. For this and other services that you would like to exempt from TOS, you can use the URL exemption field. Alternately, if you know that you only want to require TOS for a small set of URLs in total, you could list them in the URL required-match field.

### *Testing your configuration*

Now is a good time to stop and make sure everything is set up properly. Apply your changes to the ISA configuration (and then remember to wait until all Array members are synchronized, if you are running Enterprise edition).

When you direct a web browser to one of your externally published servers whose listener is configured for TOS, you should receive a simple "extranet" TOS

page.

If you have configured your Internal network for TOS, you should be able to use a browser on the Internal network to reach an outside third party web site, and be presented with a simple “network” TOS page.

# Customizing WebTOS

### *Support statement*

Note: Collective Software support is always happy to help get you started with your customizations. Two example TOS pages are provided in the installation. Before reporting a bug against WebTOS, please test using the example setup that comes with the filter, instead of your own customized page. This ensures that the problem is not due to a bug in the customization. Collective Software support cannot be responsible for troubleshooting customer-created DHTML and/or code.

### *Location and types of TOS files*

WebTOS serves all TOS-related files (DHTML and images) from one fixed directory. If you have installed ISA in the default location, then this directory will be C:\Program Files\Microsoft ISA Server\Collective Software\WebTOS\HTMLFiles. Please note the following limitations:

- **If you are on an Enterprise array, you must put identical files on each server** in the HTMLFiles directory. Otherwise, different requests might receive different TOS screens!
- You cannot create subdirectories under this folder, nor can you serve files from other directories on the ISA server (although you could still make absolute HREFs to files hosted on some other server that's not behind the WebTOS realm).
- The following file extensions are supported: html, htm, jpg, jpeg, gif, png, css, js.
- No ASP or other server-side scripting or processing is supported (client side javascripts will work, however).

These limitations are for security purposes, and the last point is simply due to the fact that ISA is not a full-featured web server that can support server-side scripting technologies.

### File Names

The names of the files in the HTMLFiles directory are significant and should not be changed. For example, WebTOS will always use the file named “TOS_proxy.htm” to serve the Internal network TOS form (“TOS_published.htm” for the external network form). You may still create other html files (if you wish to

serve them via an Iframe or frameset) but the original file names will always be referenced and served by WebTOS.

### Default files

When you first install WebTOS, a set of default files is created in the HTMLFiles directory. These are:

- TOS_proxy.htm
- TOS_published.htm
- default.css
- Several GIF files

You may modify these files and your changes will always be saved (the installer will never delete or overwrite these files once they have been created).

### Example files

There are several example files, which begin with "example_". These files are for example purposes only, and are not used in the filter. **The files will be overwritten and/or removed whenever the installer is run.**

### TOS html pages

The provided htm pages are extremely basic forms that demonstrate how to create a page that can be served by WebTOS. Any HTML may be used in this file, as long as the form POSTs back to the same page (this is how WebTOS detects that the user has agreed). See the comments in the example pages for further information.

### *Supporting files*

Images, stylesheets, and javascripts may be stored in the HTMLFiles directory and referred to with relative URLs. Keep in mind that you may not serve files from subdirectories or superdirectories, only the "HTMLFiles" folder itself. If you have a large number of users, keep in mind that serving big graphics files will substantially slow down the loading of the login page. All HTML served by WebTOS must be processed through the filter thread itself, and caching features are not supported for this content.

### *Additional Information*

A discussion about DHTML is outside the scope of this document. For complex DHTML programming tasks, we have found the O'Reilly Dynamic HTML reference to be invaluable.

## Requests

Thank you for evaluating WebTOS; we hope it meets the needs of your organization!  If you have any feature requests or other comments, please address them to info@collectivesoftware.com.

# Appendix A: Regular Expressions

A full discussion of regular expression syntax is beyond the scope of this document. WebTOS supports perl-compatible extensions to standard regular expressions. All WebTOS regular expressions are case-insensitive automatically.

Most users will only be interested in very simple expressions. To match several strings “foo”, “bar”, and “zed”, you can use the alternation operator '|' as follows:

```
foo|bar|zed
```

Which means requests matching any one of these strings will trigger the exemption.

In regular expression syntax, a period represents one wild card character. In other words, a period will match exactly one character, but it doesn't matter what that character might be (hence it's a wild card). To get the more customary “as many characters as you want” wild card, you append an asterisk after the period. So:

```
Before.*After
```

would match any string that contains “Before”, followed by 0 or more characters, followed by “After”.

There are many fine tutorials online that go into far more detail about regular expressions. A quick web search will bring up several examples, including

- http://www.regular-expressions.info/
- http://www.cc.gatech.edu/classes/RWL/Projects/citation/Docs/Design/regex.intro.1.doc.html

and many others.

Finally, if you know what perl extensions to regex are, then you clearly don't need for them to be explained in detail here. Of primary interest are:

- non-greedy quantifiers
- look-ahead and behind constructs
- etc.

See http://linuxcommand.org/man_pages/perlrequick1.html for more on perl regex.