# PageGuard Documentation

(The following graphics are screen shots from Microsoft® ISA Server 2006 and TMG which are the property of Microsoft Corp. and are included here for instructive use. Some images illustrate PageGuard, which is the property of Collective Software.)

## Table of Contents

## Problem: You want to limit access to published web sites, but not have to use HTTPS for the whole site

- Your organization uses ISA Server 2006 or TMG 2010 in a “reverse proxy” scenario for publishing internal web sites.
- Your sites are not anonymously available, you require authentication to Active Directory domain through ISA/TMG before connections are allowed to your web servers.
- For security, you use form-based authentication through ISA/TMG, and this must be over SSL to prevent plain text disclosure of credentials.
- In general, the content of your published sites is not confidential enough to merit an ongoing SSL connection after authentication.
- You may have certain content that should always be served over a secure link, even if it is requested through an unsecure link.

### Problems

- ISA 2006 and TMG can upgrade connections to HTTPS when authentication is required, but they do not support downgrading from HTTPS to HTTP after an authenticated session has been securely established.
- Using HTTPS for all parts of your published infrastructure may cause unacceptably high CPU usage on your server, or require the purchase of several certificates.
- There is no easy way to use link translation to force certain links from HTTP to HTTPS (or vice versa).

## Solution

PageGuard from Collective Software augments the capabilities of ISA 2006 and TMG 2010 to allow HTTP site publishing with HTTPS authentication.  PageGuard integrates into ISA/TMG to seamlessly solve protocol redirection, without resorting to scripts or other changes on your web servers.

### Features

- PageGuard can protect the authentication dialog on a dual HTTP/HTTPS listener and require login over HTTPS, without requiring all parts of the site to use HTTPS.
- PageGuard can specify certain publishing rules, URLs, and/or file extensions that should always be served over HTTPS.  This flexibility allows you to protect certain content or pages such as:
    - Sensitive documents
    - Secondary login forms of your internal servers that should be served over HTTPS when being transmitted over the Internet.

- PageGuard can specify certain publishing rules, URLs, and/or file extensions that should always be served over HTTP.  This allows you to “force” connections to go to HTTP after authentication is completed, or after an HTTPS page has been viewed.

### Requirements

- ISA Server 2006 or Threat Management Gateway 2010
- Microsoft .NET Framework version 2 should be installed on each ISA/TMG server.

### Caveats

- For high security sites, always use HTTPS for the whole site.
- If you use the filter's demo version in your production environment and let the evaluation period expire, PageGuard functionality will stop working and ISA/TMG will begin serving authentication pages without HTTPS protection!  See the Licensing section.  If you stop using the filter, please uninstall it and configure your sites for normal HTTPS publishing for best security.
- Any traffic transmitted over unencrypted HTTP may be subject to eavesdropping attacks, particularly over open WiFi networks.  Before implementing this solution, please understand the confidentiality level of your published sites and what the security requirements of your organization are with respect to disclosure.
- Form authentication has the option “Ignore browser IP address for cookie validation”.  Do not use this setting with dual HTTP/HTTPS sites!  If you do, then an attacker can eavesdrop an authenticated user and steal their session credentials.  This means that for the session duration the attacker can make any requests as if they were the real user.  Even though the attacker does not discover the user's password in this attack, it is still an important vulnerability and should be well understood!

## 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 of PageGuard

## *Install Procedure*

1. Close the ISA/TMG management console if it's open.
2. Execute the PageGuard_Win32.msi file (on ISA) or PageGuard_x64.msi file (on TMG). This will stop your firewall service, install the filter and interface software, register the filter, and then re-start the firewall service.
3. If you are installing over a remote desktop session, keep in mind that when the firewall service stops and restarts your RDP connection may be frozen, dropped or timed out. If an error occurs during the installation and the firewall service cannot be restarted, you will need to access the console to troubleshoot further (see below).
4. You must run the installer on each firewall server in an array separately, so they will all have the filter files installed and registered.
5. If the installation completes with no errors, then you can proceed to the configuration section.

## *Troubleshooting*

The installation normally completes without errors. However there are a few possible failure modes that can occur for this complex install process.

### Install rolls back (with red error message at the end)

If you are presented with an error message on the final screen, then check out the application event log, which often will contain details on why the installation failed. The problem may be immediately solvable from this information, or you may need to work with Collective support for additional troubleshooting assistance.

### Frozen or hung install

The installer tries to start the firewall service after it is done registering the filter components. In rare cases, everything may register properly but there could still be a problem preventing the firewall service from starting. In this situation, the installation may appear to hang on the “Starting services...” item. This is because it is trying repeatedly to start the service, and failing. In fact if you look at the application event log, you will see several errors from the firewall service as it tries to start. These messages may help identify the cause of the problem.

The install should eventually give up on starting the service, but it may take a long time. If necessary, you can expedite the rollback by going into the services control panel and setting the Microsoft Firewall service to Disabled temporarily (and applying that change). This will cause the installer to quickly give up, and it should then correctly roll back the installation while leaving the firewall service down. After this happens you can then re-enable and restart the firewall service.

This kind of problem should not normally occur, and will probably require additional troubleshooting by Collective support.  However if you are able to fix the problem you can re-run the install safely after completing this procedure.

## Configuring an HTTP site to use HTTPS authentication

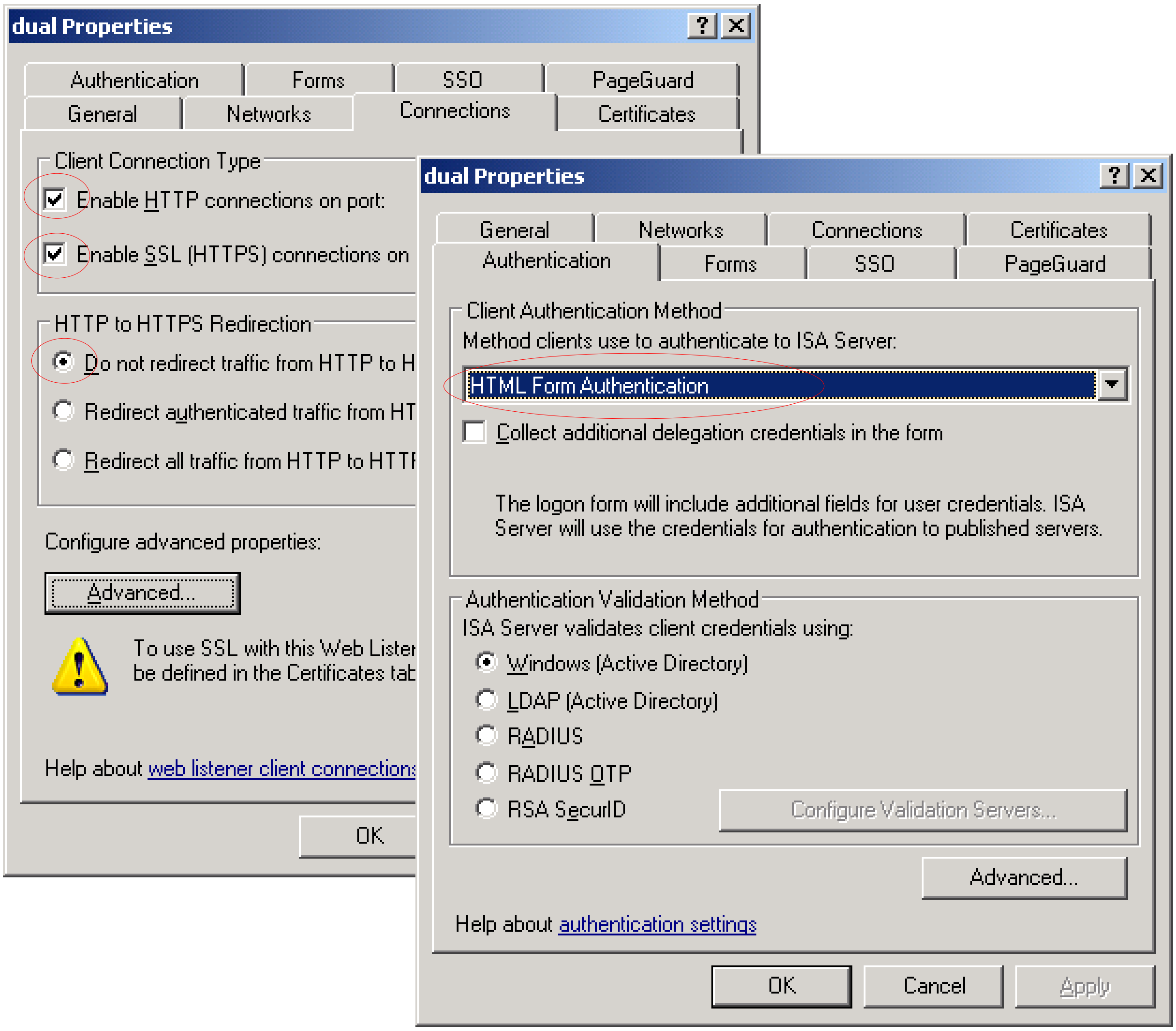
As with any published site, you will need a Listener, and one or more Publishing Rules.

For example purposes, you may see below that we have published the site “forums.isaserver.org” as if it was a site on our intranet.  We require authentication at ISA before access to this site is allowed.

*Note: For this example to work, the client browser would have to resolve the site forums.isaserver.org to the external IP address of our ISA/TMG server.  We have done this with an entry in the client's hosts file.  This is just for testing!  For* real *sites published on your ISA/TMG server (as with all published sites), it is expected that you have set DNS properly for outside clients to resolve your site to ISA/TMG.*

## *Dual listener*

Your listener needs to accept both HTTP and HTTPS, and use Form authentication.  Do not ask the listener to do any redirection, because PageGuard will handle that in a later step.



dual Properties

Client Connection Type

☑ Enable HTTP connections on port:

☑ Enable SSL (HTTPS) connections on

HTTP to HTTPS Redirection

● Do not redirect traffic from HTTP to H

○ Redirect authenticated traffic from HT

○ Redirect all traffic from HTTP to HTTI

Configure advanced properties:

To use SSL with this Web Lister
be defined in the Certificates tab

Help about web listener client connections

dual Properties

Client Authentication Method

Method clients use to authenticate to ISA Server:

HTML Form Authentication

□ Collect additional delegation credentials in the form

The logon form will include additional fields for user credentials. ISA Server will use the credentials for authentication to published servers.

Authentication Validation Method

ISA Server validates client credentials using:

● Windows (Active Directory)

○ LDAP (Active Directory)

○ RADIUS

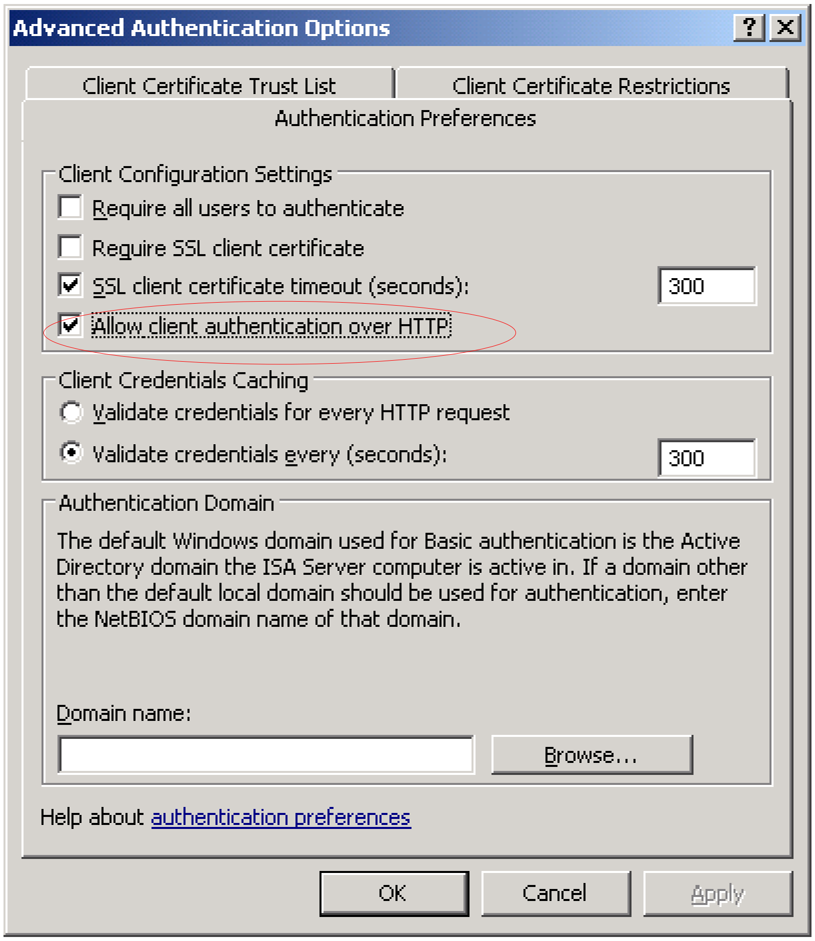
○ RADIUS OTP

○ RSA SecurID

Help about authentication settings

### *Disable HTTP check*

ISA/TMG has an extra check that forbids any part of an authenticated site from being served over HTTP.  You must explicitly disable this check to proceed further.  We will configure PageGuard to protect the authentication step later.


Advanced Authentication Options
?
Client Certificate Trust List
Client Certificate Restrictions
Authentication Preferences
OK
Cancel
Apply

Client Configuration Settings

☐ Require all users to authenticate

☐ Require SSL client certificate

☑ SSL client certificate timeout (seconds): 300

☑ Allow client authentication over HTTP

Client Credentials Caching

○ Validate credentials for every HTTP request

● Validate credentials every (seconds): 300

Authentication Domain

The default Windows domain used for Basic authentication is the Active Directory domain the ISA Server computer is active in. If a domain other than the default local domain should be used for authentication, enter the NetBIOS domain name of that domain.

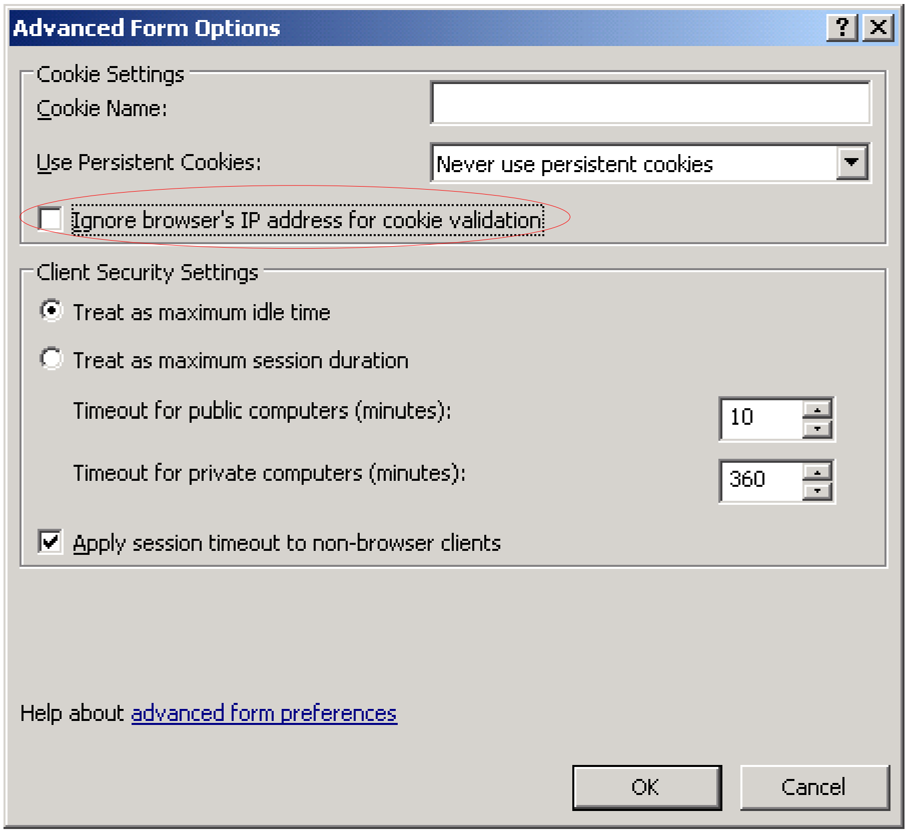
Domain name:

Browse...

Help about authentication preferences

### *Enable IP address matching for cookie validation*

Make sure you have this value **unchecked** in the advanced form options, to prevent hijacking of authenticated sessions (see Caveats section):



Advanced Form Options

Cookie Settings

Cookie Name:

Use Persistent Cookies: Never use persistent cookies

□ Ignore browser's IP address for cookie validation

Client Security Settings

● Treat as maximum idle time

○ Treat as maximum session duration

Timeout for public computers (minutes): 10

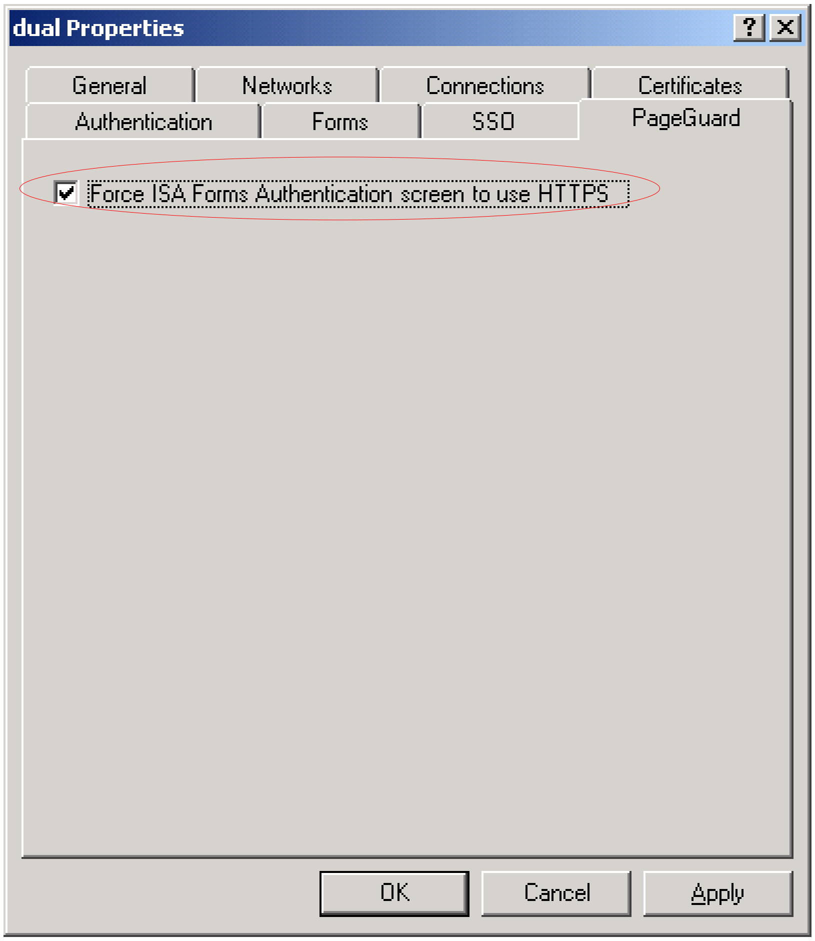
Timeout for private computers (minutes): 360

☑ Apply session timeout to non-browser clients

Help about advanced form preferences

### *Enable PageGuard to protect the form authentication page*

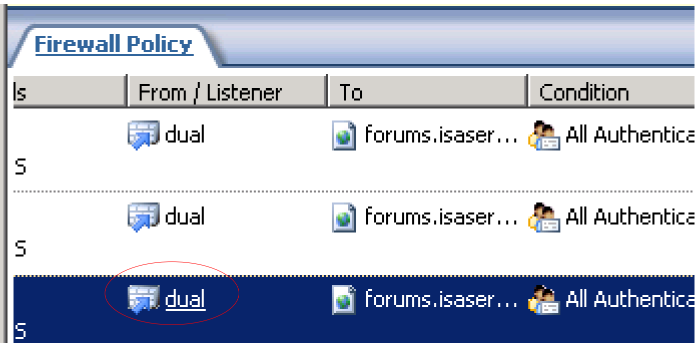
Above, recall that we had to disable the built-in logic for forcing HTTPS authentication, because it would also prevent serving the rest of our content over HTTP later.  But we still definitely want the authentication pages to be HTTPS.  So select this option in the PageGuard tab:



☑ Force ISA Forms Authentication screen to use HTTPS

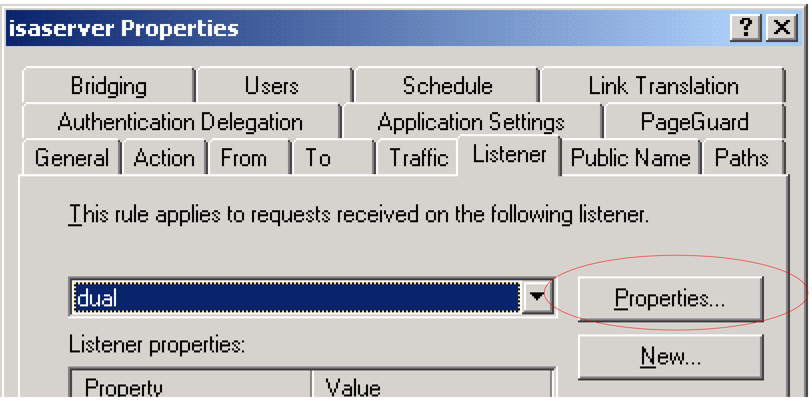
Now, even though the proxy believes it is being allowed to serve the authentication form over HTTP, PageGuard will step in to redirect the browsers to HTTPS whenever the authentication page needs to be shown.

Note: If you do not see the "PageGuard" tab, it may be because you opened the Listener dialog by clicking here, in the web rule line:



| ls | From / Listener | To | Condition |
|---|---|---|---|
| S | dual | forums.isaser... | All Authentica |
| S | dual | forums.isaser... | All Authentica |
| S | dual | forums.isaser... | All Authentica |

Or here, in the rule dialog:

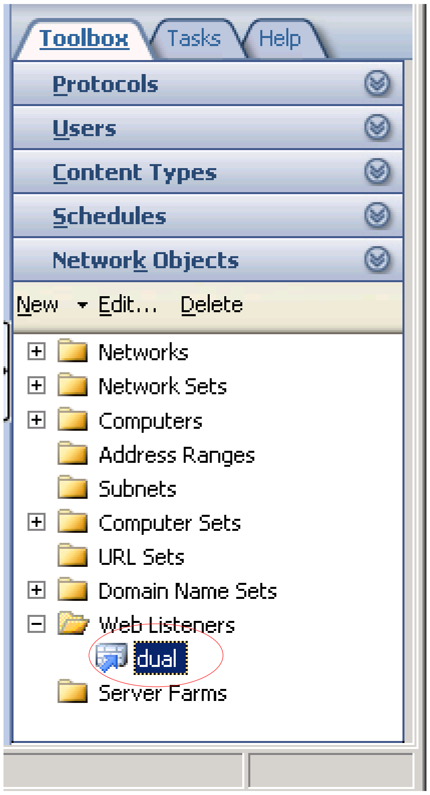


This rule applies to requests received on the following listener.

dual

Listener properties:

Due to a bug in the ISA/TMG console, custom tabs cannot be shown when the Listener dialog is opened this way. Instead, you **must** access the listener from the Toolbox area on the right:

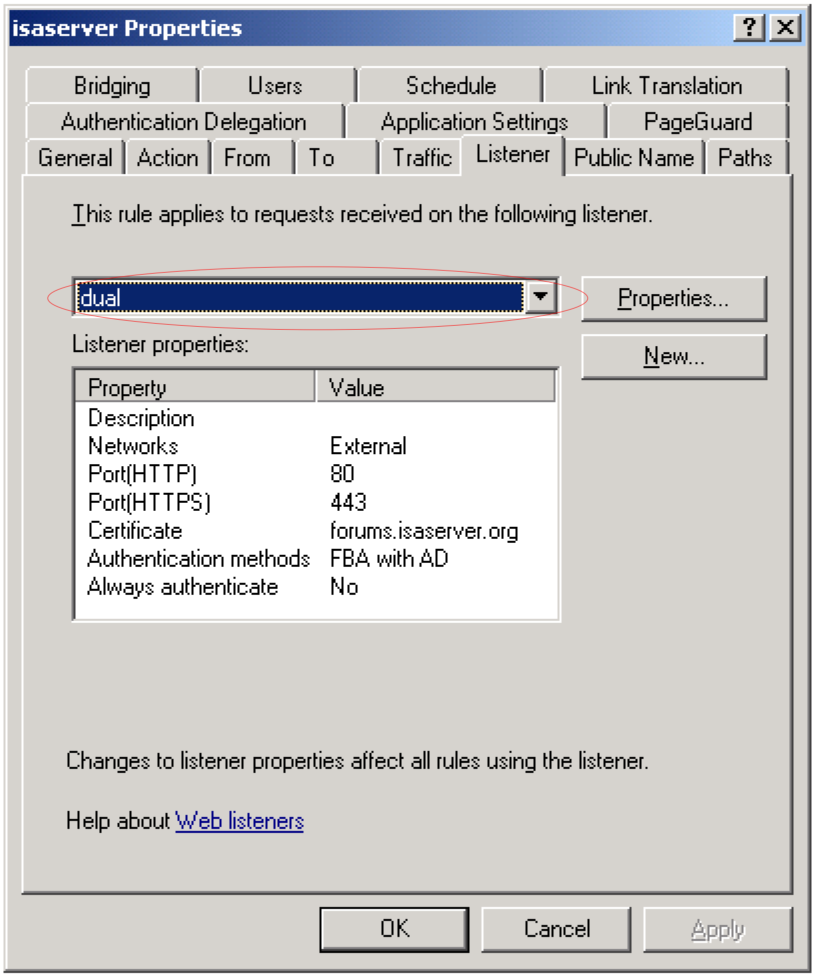


OK, if you didn't do this, you need not panic. Just select “OK” to save your changes, then re-open the dialog from the Toolbox to get access to the the “hidden” PageGuard tab.

We are now done configuring the Listener properties.

### *Configuring the Web Publishing rule for our HTTP site*

Make sure your rule is using the listener you configured above:



This rule applies to requests received on the following listener.

dual

Listener properties:

| Property | Value |
|---|---|
| Description | |
| Networks | External |
| Port(HTTP) | 80 |
| Port(HTTPS) | 443 |
| Certificate | forums.isaserver.org |
| Authentication methods | FBA with AD |
| Always authenticate | No |

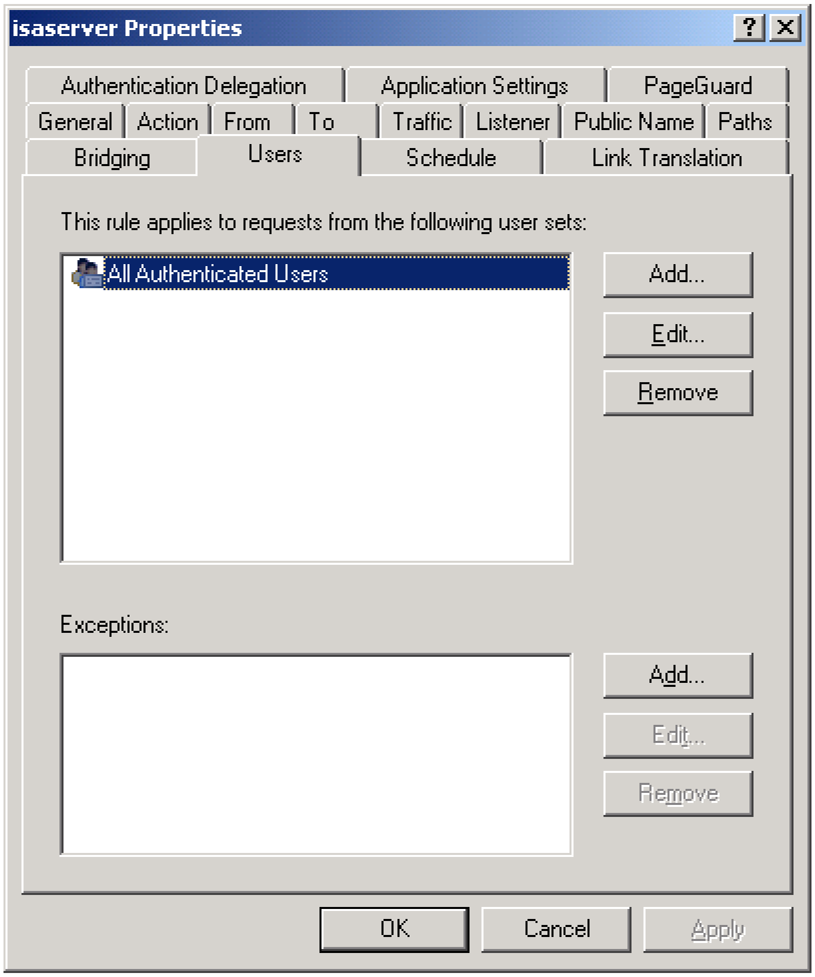
Changes to listener properties affect all rules using the listener.

Help about Web listeners

If you don't use a dual listener, then the PageGuard redirection can fail, and your authenticated session cannot be used to get access to content served over HTTP.

### *Require authentication*

In order for ISA/TMG to trigger authentication for this rule, be sure the Users list **does not** specify the “All users” set:



isaserver Properties

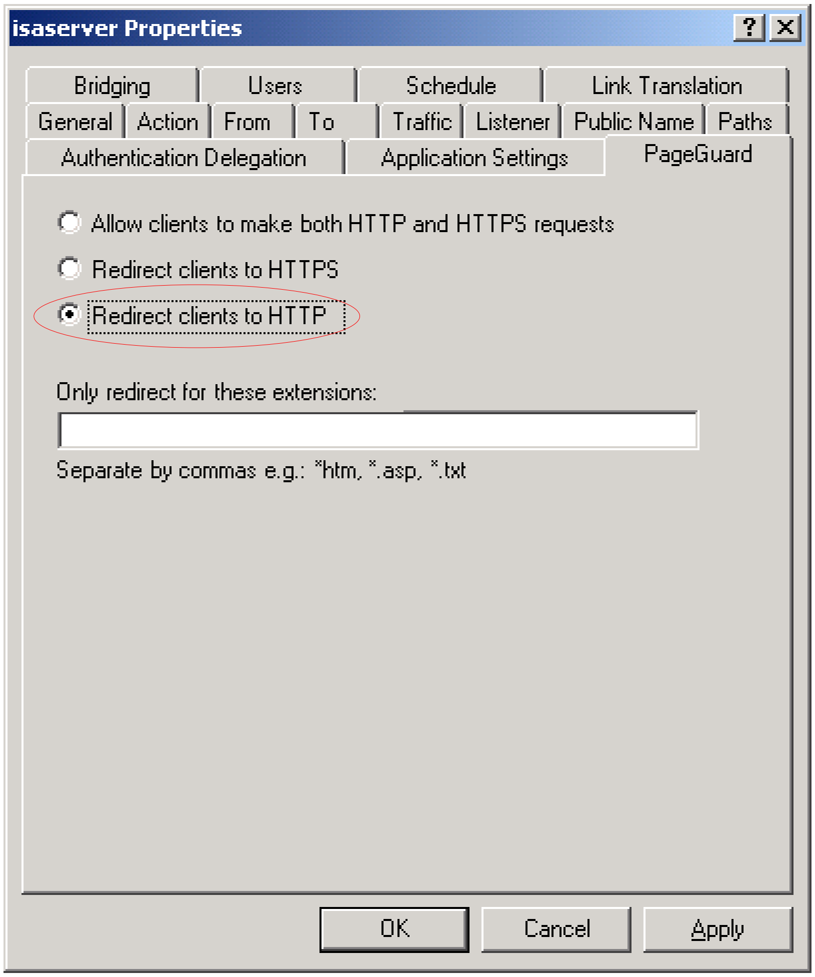
This rule applies to requests from the following user sets:

All Authenticated Users

Exceptions:

### *Specify the whole site as HTTP*

All pages of this site should be HTTP, so in the PageGuard tab, select “Redirect clients to HTTP”.  This ensures after secure authentication the user is returned to normal HTTP mode.



○ Allow clients to make both HTTP and HTTPS requests

○ Redirect clients to HTTPS

● Redirect clients to HTTP

Only redirect for these extensions:

Separate by commas e.g.: *htm, *.asp, *.txt

If you do not use this setting, once users are in HTTPS for authentication, they would “stay” there, thus defeating the purpose of this PageGuard scenario.

### *Testing the HTTP site with HTTPS authentication*

After applying your configuration (and synchronizing, if Enterprise edition),

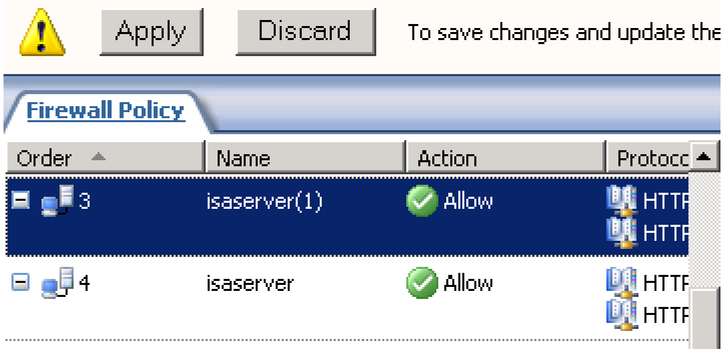
- Close all browsers.
- In a new browser, visit the published site by typing in the HTTP version of the URL.
- ISA/TMG should show the Form for logon; PageGuard should seamlessly redirect the form to be served as HTTPS.
- Log in with a valid identity that is allowed by your publishing rule.
- The page you requested should now be served; PageGuard should seamlessly redirect the requested page to be served as HTTP.
- If you request pages on the site explicitly with HTTPS, PageGuard should seamlessly redirect them to be served as HTTP.

# Adding some HTTPS protected items

Here we will build on the above scenario, and additionally specify that some items on the site are always to be served via HTTPS, even if they are requested with HTTP links. Please understand and implement the above scenario before adding this one.

## *A new specific rule*

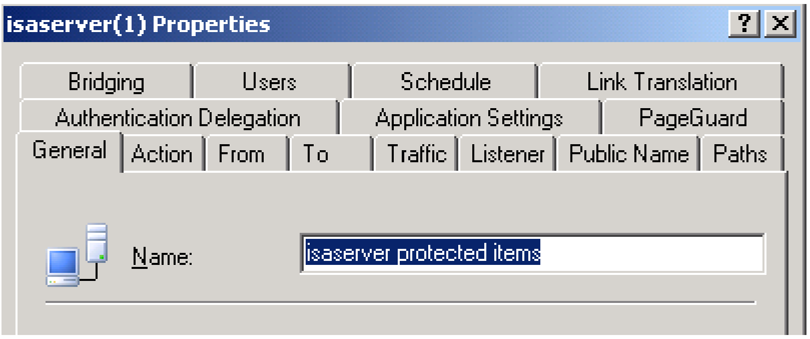
Create a new publishing rule by right-clicking the existing rule, selecting Copy. Then right click and select Paste:



| Order | Name | Action | Protoco |
|---|---|---|---|
| 3 | isaserver(1) | Allow | HTTP<br>HTTP |
| 4 | isaserver | Allow | HTTP<br>HTTP |

The new rule should appear above the old one, and have a (1) in the name to make it unique. **If the rule is not above the old one, then move it up.** We will make some “narrow” (specific) changes to the Paths tab of the new rule, and it must apply before the more “general” /* rule for the whole site.

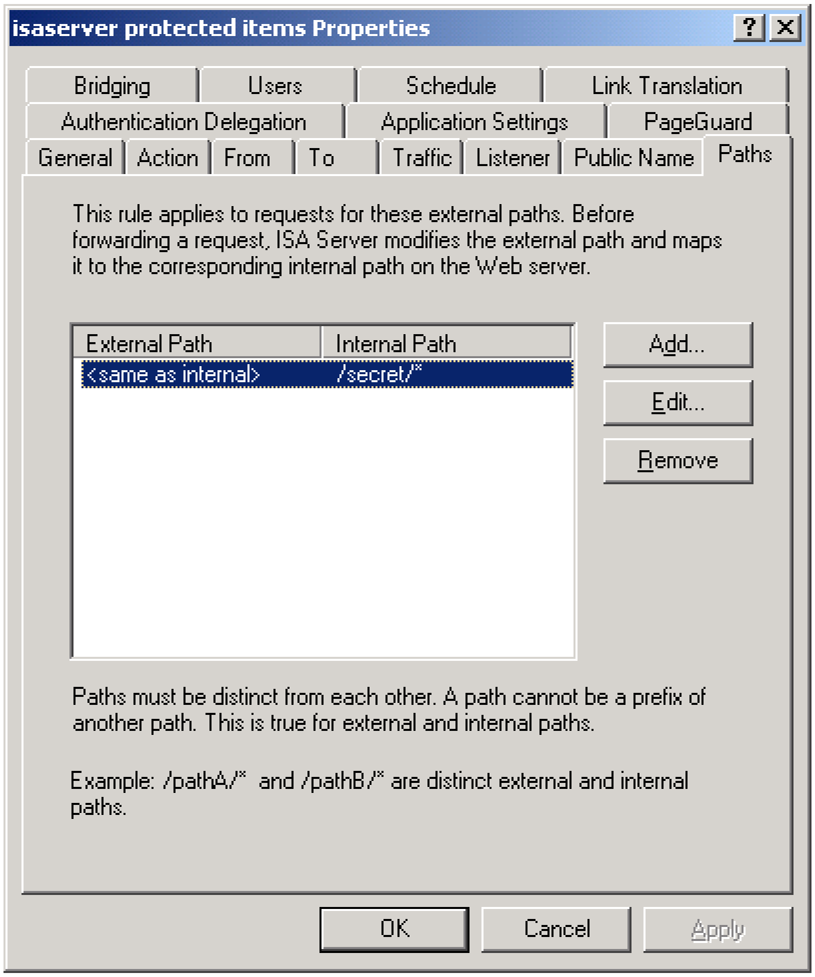
Go into the rule and give it a better name:



Name: isaserver protected items

### *Narrow the rule scope*

Instead of /*, we will make this rule apply to only a certain path on the web server.  The one that contains our secret documents:



This rule applies to requests for these external paths. Before forwarding a request, ISA Server modifies the external path and maps it to the corresponding internal path on the Web server.

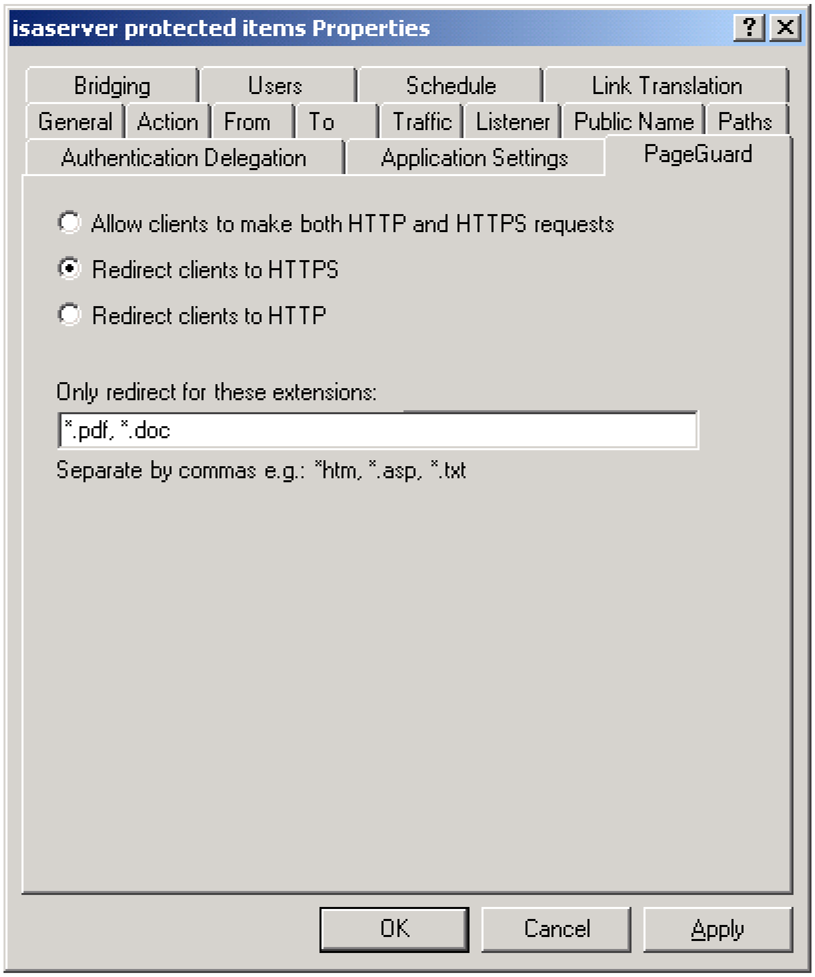
| External Path | Internal Path |
|---|---|
| <same as internal> | /secret/* |

Paths must be distinct from each other. A path cannot be a prefix of another path. This is true for external and internal paths.

Example: /pathA/*  and /pathB/* are distinct external and internal paths.

### *Force some extensions to HTTPS*

In this “secret” rule, we can tell all .pdf and .doc links to be forced to HTTPS:



○ Allow clients to make both HTTP and HTTPS requests

● Redirect clients to HTTPS

○ Redirect clients to HTTP

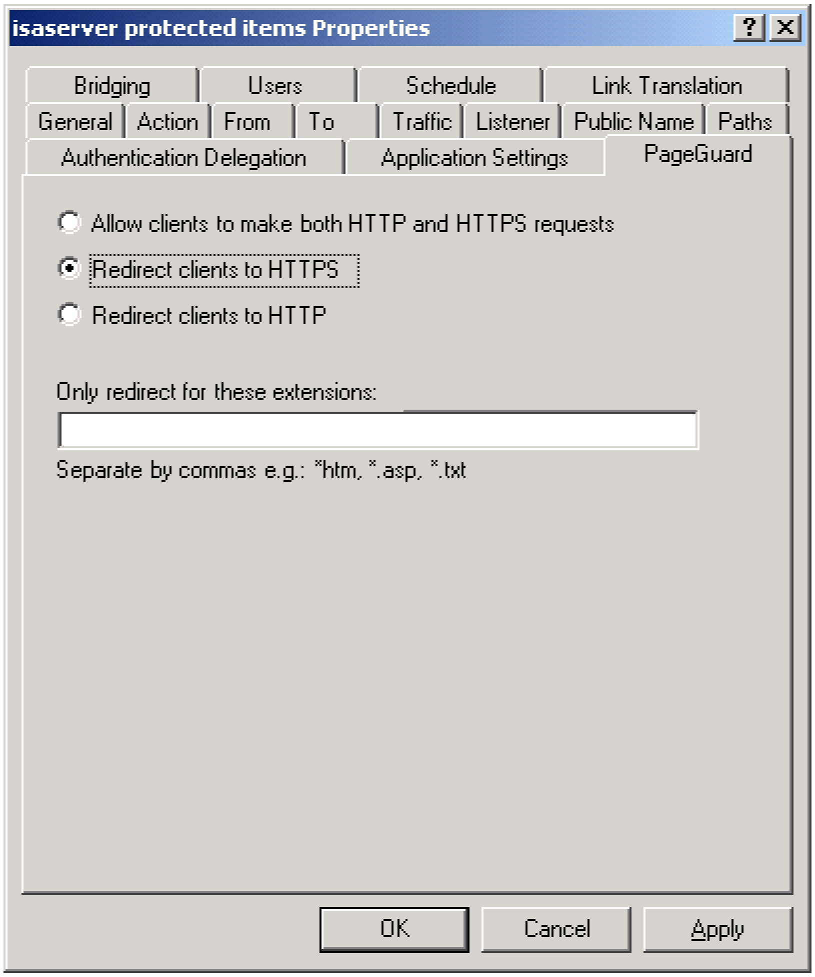
Only redirect for these extensions:

*.pdf, *.doc

Separate by commas e.g.: *htm, *.asp, *.txt

### *Or, force everything in the path to HTTPS*

Here is an alternate configuration that protects all requests within the “/secret/*” part of the site.



○ Allow clients to make both HTTP and HTTPS requests

● Redirect clients to HTTPS

○ Redirect clients to HTTP

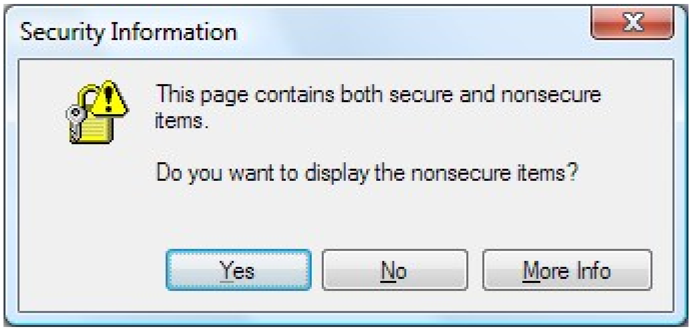
Only redirect for these extensions:

Separate by commas e.g.: *htm, *.asp, *.txt

Notice we leave the extensions field empty to mean “every request that matches this rule”.

### *Dealing with “nonsecure items” warnings:*

Publishing a site that has both HTTP and HTTPS parts can yield some odd results. If you use PageGuard to serve some pages as HTTPS, you may see the following popup during your testing of those pages:



Security Information

This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

This means that some items loaded on the HTTPS page are requested using the HTTP protocol. Why? There are a couple possible reasons for this to be the case:

- There may be content (images, ads, CSS, scripts) served from other, non-secure sites. If that content's site does not support HTTPS, then there is not much you can do for this. (If the whole page does not need to be in HTTPS, but only some types of documents that you serve from links on the page, you can use this configuration instead.)
- The content may be served with an HTTPS link properly, but the request may be matching the /* rule we configured in the first scenario. Well, that rule forces *every* matching request to be served as HTTP! Let us examine this problem further below.

The root cause may be that you have certain resource items (your logo, stylesheets, etc.) that must be served at different times as HTTP and as HTTPS, depending on the protocol of the requesting page. For these items we don't really care about which protocol is used, as long as the site works right without errors!

Now, if these “don't care” items are in known specific paths that can be treated separately from the other paths, you can create a new publishing rule, between the others, to handle them. So the rule order would now be:

1. **Protected items** rule with path “/secret/*”: PageGuard forces pages to HTTPS.
2. **Don't care** rule with path “/images/*”, “/css/*” etc.: PageGuard set to “Allow clients to make both HTTP and HTTPS requests”.
3. The **main rule** for the site with path “/*”: PageGuard forces pages not covered by the other 2 rules to go to HTTP.

Order is important! The more general (/*) rules should always be placed lower than the specific ones (/images/*).

There is a different way to approach this problem as well, which may be easier depending on your configuration. See next section for details.

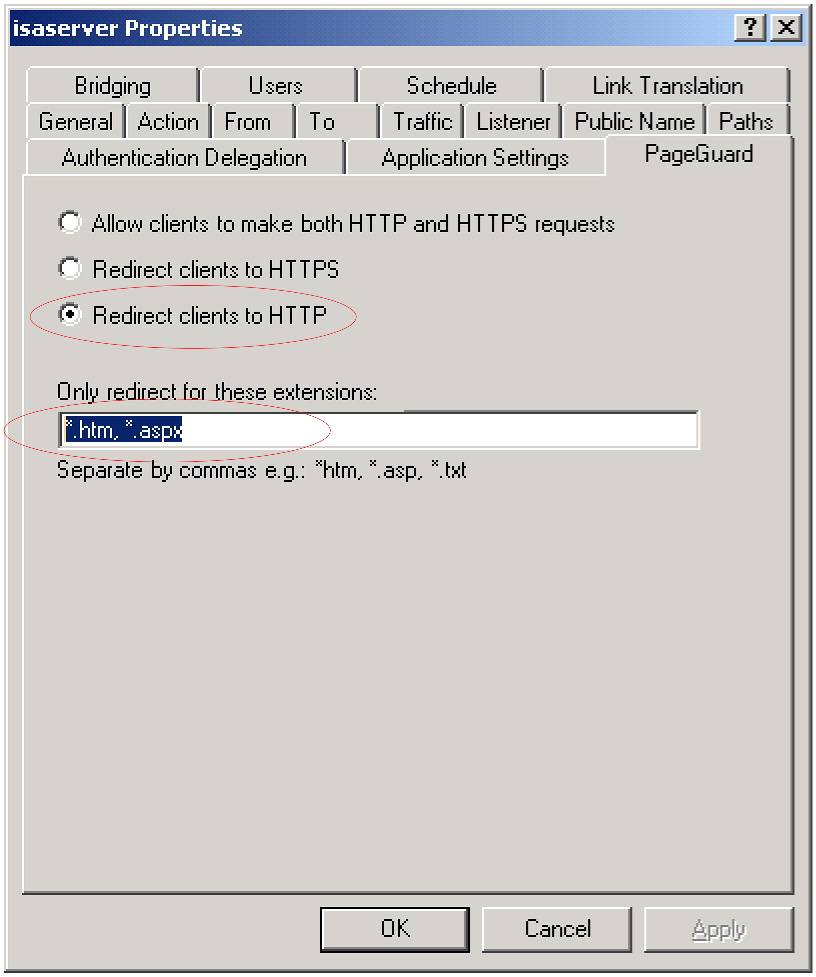
### *Making the main /* rule smarter*

In the first scenario we considered a 100% HTTP site, so asking PageGuard to redirect all requests to HTTP was fine.  But this may not be appropriate when your site has a mix of HTTP and HTTPS.

When an HTML page is served, the Link Translation feature will automatically convert the URLs to be the same protocol as the page.   So other items like images and scripts will naturally be requested in the same protocol as the page itself.

With this knowledge, you can see that PageGuard may be constrained to only consider certain types of requests, and leave alone all the others without redirecting them.

If you know the extensions of your web pages that will be requested (.html, .asp, .php, etcetera) then you may configure the main /* rule as follows:



○ Allow clients to make both HTTP and HTTPS requests

○ Redirect clients to HTTPS

● Redirect clients to HTTP

Only redirect for these extensions:

*.htm, *.aspx

Separate by commas e.g.: *htm, *.asp, *.txt

In this fashion, the redirection will still occur when the user requests .htm and .aspx pages, but PageGuard will allow other requests (for images and other extensions) to be served with either protocol, without interfering.

So if you are able to use this solution, you do not need a rule for “don't care” items, because we have handled that case here in the /* rule.

In the next section we will deal with default pages (URLs with no extensions)

### *What about “sections”, index pages, URLs with no extensions?*

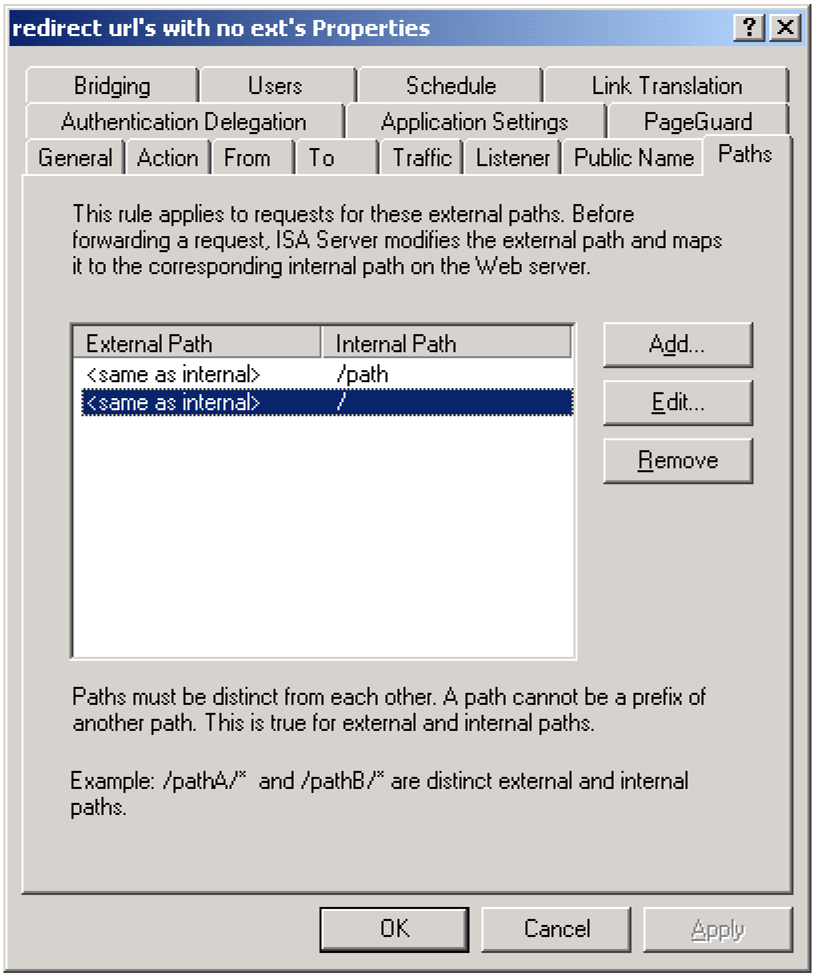
If you follow the above section and make the HTTP redirection happen only when certain extensions are requested, there is a problem with URLs of the form:

- example.com/
- example.com/path/

where no extensions are used. If your whole site uses this paradigm, then the extension feature may not be useful to you. If however there are only a small, known number of URLs of this form that will be used as portals or main access points, you can still tell PageGuard to redirect them.

Create a new rule (again a copy, as we did in this section).

This rule's position should be **above the /* rule** so it matches first. In the paths tab, add exactly the paths (without *'s) that you want to redirect:



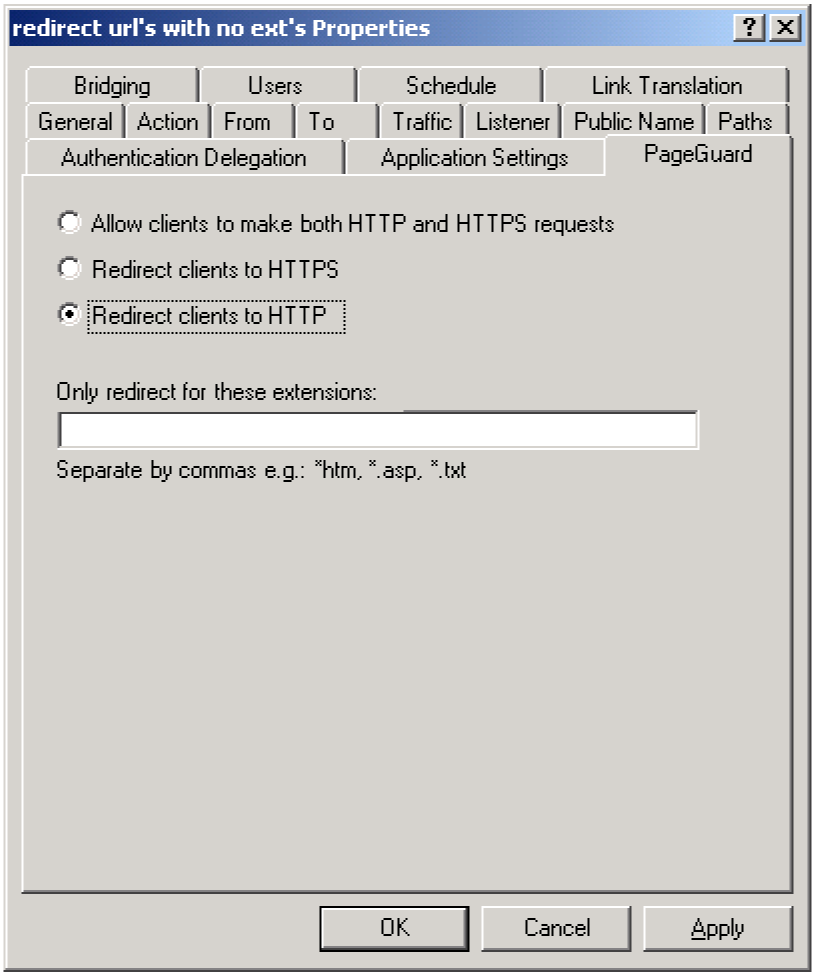
This rule applies to requests for these external paths. Before forwarding a request, ISA Server modifies the external path and maps it to the corresponding internal path on the Web server.

| External Path | Internal Path |
|---|---|
| <same as internal> | /path |
| <same as internal> | / |

Paths must be distinct from each other. A path cannot be a prefix of another path. This is true for external and internal paths.

Example: /pathA/* and /pathB/* are distinct external and internal paths.

and the PageGuard tab:



○ Allow clients to make both HTTP and HTTPS requests

○ Redirect clients to HTTPS

● Redirect clients to HTTP

Only redirect for these extensions:

Separate by commas e.g.: *htm, *.asp, *.txt

So with this rule those precise paths (but no others) will be matched, and therefore redirected to HTTP. Other requests that don't match will fall to the /* rule, whose behavior we configured appropriately in the previous section.

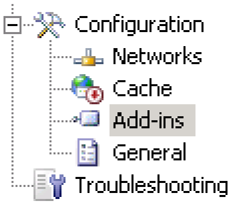
## Other configurations

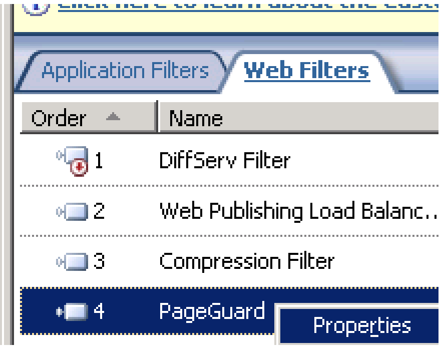
It is not the intent of this manual to cover every possible scenario for which you may use PageGuard. Rather, with these examples we try to show what types of operations the filter can perform, how it integrates into ISA/TMG, and how to set up some common uses. Furthermore the examples try to illustrate *why* the filter works the way it does. If you have questions about a different case not elaborated here, please open a support ticket on our web site and we can assist you.

Also, please use the evaluation of the filter in your test lab. Once you understand how the filter and the publishing rules operate, you can try different configurations and rule orderings to get your desired result.

## Filter licensing

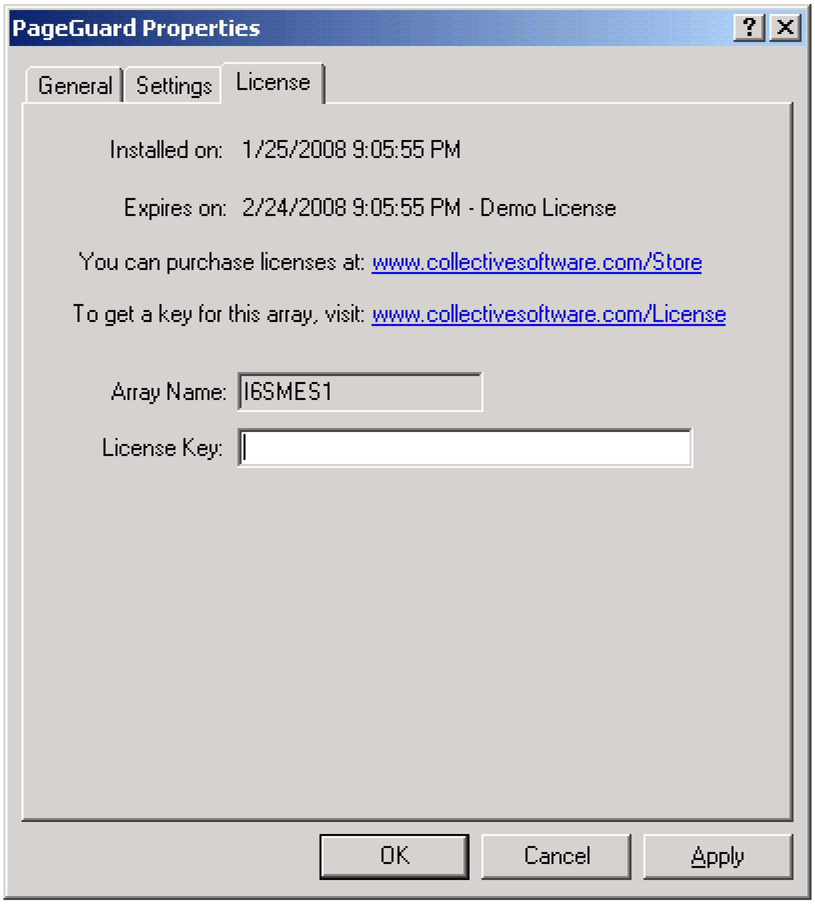
To view your evaluation period or enter a key, go to Add-ins, Web Filters, and select PageGuard properties:





| Order | Name |
|---|---|
| 1 | DiffServ Filter |
| 2 | Web Publishing Load Balanc… |
| 3 | Compression Filter |
| 4 | PageGuard |

and select the License tab:



Installed on: 1/25/2008 9:05:55 PM

Expires on: 2/24/2008 9:05:55 PM - Demo License

You can purchase licenses at: www.collectivesoftware.com/Store

To get a key for this array, visit: www.collectivesoftware.com/License

Array Name: I6SMES1

License Key:

The License tab is used to check how long remains in the evaluation period, and to activate a permanent license.

To be eligible for a license key, you need to purchase license(s). You can do this on our web store or by contacting us.

Once you have available license(s) you can request a key for your array (or single server) at our licensing page. When requesting a license key, you will need to tell us the name of the ISA/TMG array, which is indicated on this dialog. The exact name is important, because it will be used to validate the key.

The license key is sensitive to the number of servers in the array. For example if you begin with only 2 servers in the array but plan to have 4, you can purchase 4 licenses and request a license key for a 4-server array. Then as you bring future servers online, they will be licensed automatically.
**Warning:** if you install more servers than you have licensed then the license key will be seen as invalid, and the servers will begin to operate in demo/lab mode. So if you need to add more servers to a live array then you should acquire and apply your new license key in advance, so this behavior does not take place.

### *Demo/Lab mode*

When the evaluation period expires (after 30 days) or when an invalid license key is used, the filter runs in demo/lab mode. In this mode the filter will work normally for a period of 2 hours from the starting of the Firewall Service, and then stop working after that time. This mode is meant to be useful for test labs where you don't wish to purchase licenses but still want to be able to run meaningful test setups. After 2 hours, you can restart the firewall service and the lab timer will reset again.

### *Troubleshooting*

The first place to look if something seems to be working incorrectly is the Alerts tab in the Monitoring section. Often this will directly indicate the cause of the problem. This information will also be required in almost all cases if you need support.

## Support for PageGuard

Collective is proud to offer support for PageGuard, whether you need help getting a configuration working, find a bug, or just have a feature question.

Support is available from our web site at http://www.collectivesoftware.com/Support/

- *Knowledge Base*: When our staff answers questions that will apply to the whole community, they will often create a permanent KB item to disseminate this knowledge. There is a Search feature here; you can also easily browse by topic. To get fast answers to FAQs (frequently asked questions) the knowledge base is the best place to start.
- *Support ticket*: We are always happy to help you get 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.