



# WebDirect Configuration Guide

(The following graphics are screen shots from Microsoft® ISA Server 2004/2006 which is the property of Microsoft Corp. and are included here for instructive use. Some images illustrate WebDirect, which is the property of Collective Software.)

## Table of Contents

<a href="#">WebDirect Configuration Guide.....</a>	<a href="#">1</a>
<a href="#">    Problem Statement.....</a>	<a href="#">1</a>
<a href="#">    Solution Overview.....</a>	<a href="#">2</a>
<a href="#">    WebDirect Installation.....</a>	<a href="#">2</a>
<a href="#">    Publishing the real server via HTTPS.....</a>	<a href="#">3</a>
<a href="#">    Publishing the HTTP Redirector Rule (ISA 2004).....</a>	<a href="#">7</a>
<a href="#">    Publishing the HTTP Redirector Rule (ISA 2006).....</a>	<a href="#">9</a>
<a href="#">    Configuring WebDirect on the Redirector Rule.....</a>	<a href="#">12</a>
<a href="#">    Advanced Path mapping.....</a>	<a href="#">14</a>
<a href="#">    OWA Redirection.....</a>	<a href="#">14</a>
<a href="#">    “Folder Moved” Scenarios.....</a>	<a href="#">15</a>
<a href="#">    Path mapping without HTTPS.....</a>	<a href="#">16</a>
<a href="#">    General path mapping rules.....</a>	<a href="#">17</a>
<a href="#">    Additional assistance.....</a>	<a href="#">17</a>

## Problem Statement

This guide is a walkthrough of how to configure an ISA 2004 server with WebDirect so that we can publish an internal server over HTTPS, and cause all requests over HTTP to redirect to HTTPS. Because we wish to map the incoming requests exactly (including the entire URL) we will need to preserve the path information across the requests. For example, take the following scenario:

- Our internal server is at IP address 192.168.6.3 and is configured to serve requests to the intranet over HTTP with the internal DNS name “example.com”
- We wish to publish this server to the internet, but secure all access over HTTPS.
- We need all requests for “http://example.com/\*” to be redirected to “https://example.com/\*” (where \* is any valid URL).
- Even trying to solve this problem via ISA Link Translation, the initial request coming in to HTTP cannot be mapped properly. Furthermore, our server generates emails with links in the form “http://example.com/etc/etc” which would ordinarily not work for access outside the firewall.

## Solution Overview

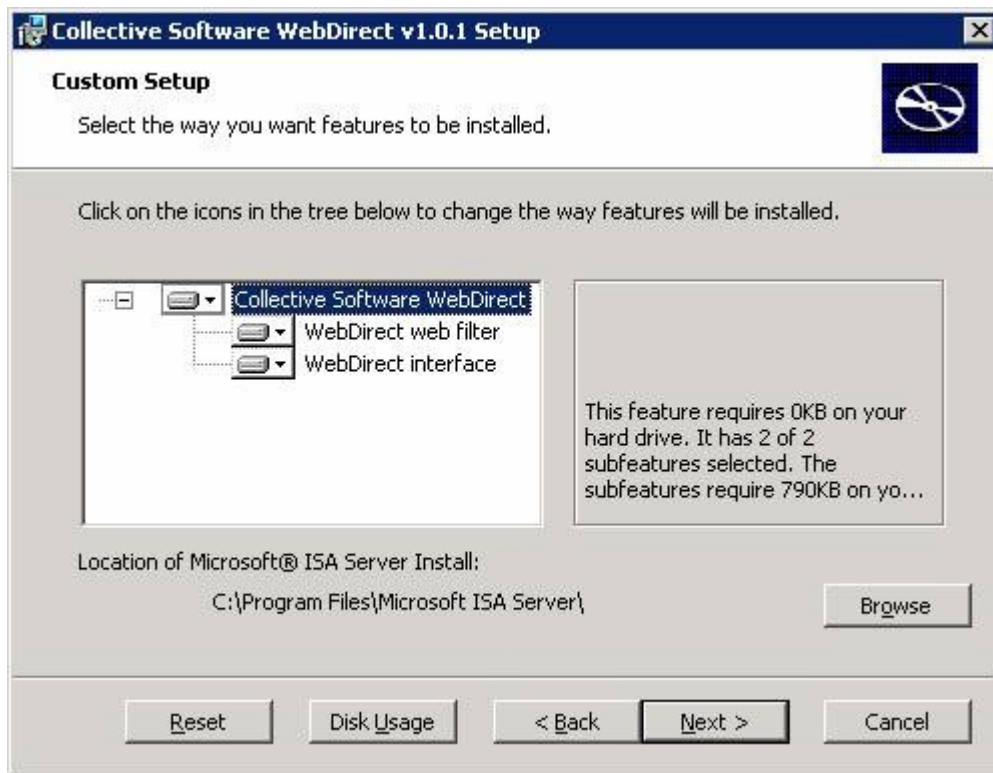
In the following sections, we will walk through setting up the WebDirect product in our ISA environment, configuring the HTTPS web server publishing rule, and then configuring a special redirector publishing rule that will match HTTP requests and redirect them to the primary publishing point.

**Note:** The only part of our ISA configuration that will be different from a standard publishing scenario is the *addition of an HTTP Redirector publishing rule*. If you already have your web publishing configuration working, then you can [install WebDirect](#) and then skip to [Publishing the HTTP Redirector Rule](#) section.

## WebDirect Installation



The WebDirect 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 “WebDirect 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 “WebDirect interface” on all machines from which you will administer your ISA enterprise. This component enhances the ISA console’s “Web Publishing Rule” properties dialog and allows you to configure the WebDirect 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.

## Publishing the real server via HTTPS

First, we need to actually publish our server so that the redirector will have a target! Select the “Publish a Secure Web Server” task from the Firewall Policy tasks panel:



Name the publishing rule (however you see fit):

SSL Web publishing rule name:

To continue, click Next.

Our real server on the intranet just serves HTTP, so we'll terminate the SSL at the ISA server by using SSL Bridging:

**Publishing Mode**  
Specify whether ISA Server inspects and filters requests to the Web site.

SSL Bridging  
ISA Server decrypts encrypted traffic and applies inspection and filtering to the content.

SSL Tunneling  
ISA Server relays unmodified encrypted traffic to the published Web server.

Our rule is to allow access:

**Select Rule Action**  
Specify how you want this rule to respond

Action to take when rule conditions are met:

Allow

Deny

Once again, the real server doesn't support HTTPS, so chose "Secure connection to clients":

**Bridging Mode**  
Specify which connections will be secured.

Secure connection to clients  
ISA Server will accept requests from clients over a secure (HTTPS) connection, and forward requests to the Web server over a standard (HTTP) connection.

Secure connection to Web server  
ISA Server will accept requests from clients over a standard (HTTP) connection, and forward requests to the Web server over a secure (HTTPS) connection.

Secure connection to clients and Web server  
ISA Server will accept requests from clients over a secure (HTTPS) connection, and forward requests to the Web server over a secure (HTTPS) connection.

Our server is at 192.168.6.3. We want the host header it receives to be "example.com" though, so we'll check the Forward option:

**Define Website to Publish**  
Specify the computer (Web server) on which the website is located. You can publish the entire website or limit access to a specified folder.

Computer name or IP address:

Forward the original host header instead of the actual one (specified above).

Enter the name of the file or folder you want to publish. To include all files and subfolders within a folder use /\*, Example: folder/\*.

Path:

Users on the internet will connect to our published server via the host name “example.com”:

**Public Name Details**  
Specify the public domain name (FQDN) or IP address users will type to reach the published site.

Accept requests for:

Only requests for this public name or IP address will be forwarded to the published site. For example www.microsoft.com.

Public name:

Path (optional):

Let’s assume we don’t have our SSL listener set up yet and do that next:

**Select Web Listener**  
The Web listener specifies the IP addresses and port on which the ISA Server computer listens for incoming Web requests.

Web listener:

Listener properties:

Property	Value

Of course we need a name:

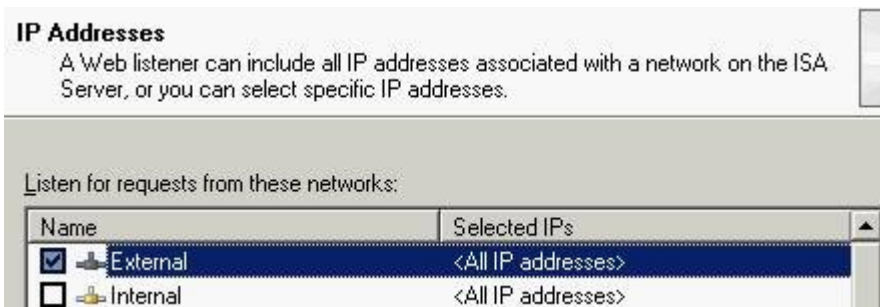
## Welcome to the New Web Listener Wizard

This wizard helps you create a new Web listener. Web listeners are used in Web publishing rules. A Web listener specifies the IP addresses and port on which the ISA Server computer listens for incoming Web requests.

Web listener name:

To continue, click Next.

In your enterprise, you will probably want to limit your listener's IP addresses, but for this example, we'll just choose all external:



**IP Addresses**  
A Web listener can include all IP addresses associated with a network on the ISA Server, or you can select specific IP addresses.

Listen for requests from these networks:

Name	Selected IPs
<input checked="" type="checkbox"/> External	<All IP addresses>
<input type="checkbox"/> Internal	<All IP addresses>

Ours will be an SSL listener:



**Port Specification**  
Specify the port that the ISA Server computer will use to listen on the selected IP addresses for incoming Web requests.

HTTP

Enable HTTP

HTTP port:

SSL

Enable SSL

SSL port:

Certificate:

You must choose your SSL Certificate at this stage. If you are working in a test environment and need some assistance getting that process going, check out this excellent MS TechNet resource for [how to grant and install a certificate](#) (specifically Appendix B may be helpful).

Now we have set up and chosen our listener, and are back to the SSL Web Publishing rule wizard. In our example, we tell ISA to allow access to anyone on the internet to access our server over SSL. (The

server itself will then authenticate them securely and allow or deny access):



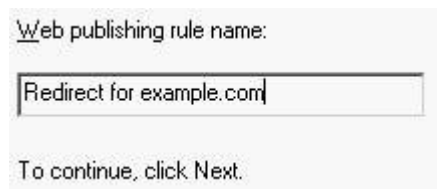
And that is the last step. After applying these changes, internet users should be able to type “https://example.com” and arrive at our server’s home page. Of course, this example assumes that you control the domain name “example.com” and have correctly pointed that DNS entry to your ISA server’s SSL listener IP address.

## Publishing the HTTP Redirector Rule (ISA 2004)

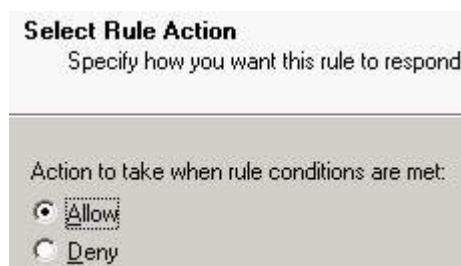
We must add a redirector rule so that any HTTP requests for example.com will be told to go to the HTTPS listener we just set up. Start by creating a Web Publishing Rule (similar to above, but not a Secure rule this time):



Give it a suitable name:



Our rule is to allow access:



We will be “publishing” a redirect to “example.com”. This screen signifies the name of the server that will be sent in the redirect request (we will see later where this appears in the WebDirect dialog):



**Define Website to Publish**  
Specify the computer (Web server) on which the website is located. You can publish the entire website or limit access to a specified folder.

Computer name or IP address:

Forward the original host header instead of the actual one (specified above).

Enter the name of the file or folder you want to publish. To include all files and subfolders within a folder use /\*. Example: folder/\*.

Path:

We want this rule to match requests for http://example.com:

**Public Name Details**  
Specify the public domain name (FQDN) or IP address users will type to reach the published site.

Accept requests for:

Only requests for this public name or IP address will be forwarded to the published site. For example www.microsoft.com.

Public name:

Path (optional):

Next, choose (or set up) a listener for HTTP. In our case we are redirecting to the same host name, so make sure the listener is set up for the same IP address(es):

**Select Web Listener**  
The Web listener specifies the IP addresses and port on which the ISA Server computer listens for incoming Web requests.

Web listener:

Listener properties:

Property	Value
Description	
Networks	External
Port(HTTP)	80
Port(HTTPS)	Disabled
Authentication methods	Integrated
Always authenticate	No

All users should be allowed to hit http://example.com in order to be served the redirect response:



**User Sets**  
You can apply the rule to requests from all users. Or, you can limit access to specific user sets.

This rule applies to requests from the following user sets:

All Users

Now we have our redirector rule all set up. But at the moment, ISA thinks that there really is a server on your intranet that answers to the DNS name of "example.com". This is where WebDirect comes in.

## Publishing the HTTP Redirector Rule (ISA 2006)

We must add a redirector rule so that any HTTP requests for example.com will be told to go to the HTTPS listener we just set up. Start by creating a Web Publishing Rule (similar to above, but not a Secure rule this time):

**Firewall Policy Tasks**

- Create New Access Rule
- Publish a Web Server**

Give it a suitable name:

Web publishing rule name:

Redirect for example.com

To continue, click Next.

Our rule is to allow access:

**Select Rule Action**  
Specify how you want this rule to respond when the rule conditions are met.

Action to take when rule conditions are met:

- Allow**  
With this option selected, incoming requests matching the rule conditions will be allowed.
- Deny**  
With this option selected, incoming requests matching the rule conditions will be denied and the traffic will be blocked.

Single web site:

### Publishing Type

Select if this rule will publish a single Web site or external load balancer, a Web server farm, or multiple Web sites.

Publish a single Web site or load balancer

Use this option to publish a single Web site, or to publish a load balancer in front of several servers.

Help about [publishing a single Web site or load balancer](#)

You can select non-secured on the next step (irrespective of whether your redirect rule will listen or redirect to https).

### Server Connection Security

Choose the type of connections ISA Server will establish with the published Web server or server farm.

Use SSL to connect to the published Web server or server farm

ISA Server will connect to the published Web server or server farm using HTTPS (recommended).



Use non-secured connections to connect the published Web server or server farm

ISA Server will connect to the published Web server or server farm using HTTP.



We will be “publishing” a redirect to “example.com”. This screen signifies the name of the server that will be sent in the redirect request (we will see later where this appears in the WebDirect dialog):

### Internal Publishing Details

Specify the internal name of the Web site you are publishing.

The internal site name is the name of the Web site you are publishing as it appears internally. Typically, this is the name internal users type into their browsers to reach the Web site.

Internal site name:

example.com

ISA Server may not be able to connect to the server hosting the published Web site unless its computer name or IP address is specified. For example, the computer name or IP address must be specified if ISA Server cannot resolve the internal site name.

Use a computer name or IP address to connect to the published server

Computer name or IP address:

Browse...

Skip the “Path” dialog for now:

**Internal Publishing Details**  
Specify the internal path and publishing options of the published Web site. You can publish the entire Web site, or limit access to a specified folder.

Enter the name of the file or folder you want to publish. To include all files and subfolders within a folder use /\*. Example: folder/\*.

Path (optional):

Based on your selection, the following Web site will be published:

Web site:

Forward the original host header instead of the actual one specified in the Internal site name field on the previous page

We want this rule to match requests for http://example.com:

**Public Name Details**  
Specify the public domain name (FQDN) or IP address users will type to reach the published site.

Accept requests for:

Only requests for this public name or IP address will be forwarded to the published site.

Public name:   
Example: www.contoso.com

Path (optional):

Based on your selections, requests sent to this site (host header value) will be accepted:

Site:

Next, choose (or set up) a **listener for HTTP**. Make sure your listener does not use authentication:

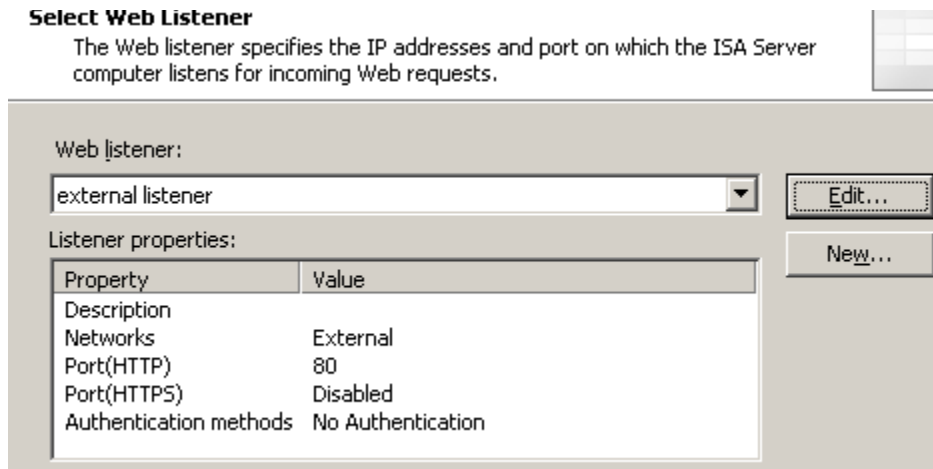
**Authentication Settings**  
Select how clients will authenticate to ISA Server, and how ISA Server will validate their credentials.

Select how clients will provide credentials to ISA Server:

When you are going to redirect HTTP to HTTPS, you should **never let the HTTP listener do authentication**. This way, you do not risk sending credentials unencrypted. (The HTTPS listener will

do your authentication after the redirection has taken place). The key to remember is that the HTTP traffic will be “caught” at ISA server and bounced back to the browser with a redirect command. Therefore it is not necessary to authenticate or secure this traffic, as it will never “get past” the firewall into your organization.

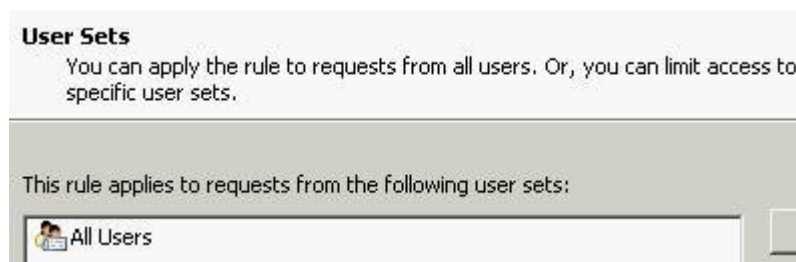
In our case we are redirecting to the same host name, so make sure the listener is set up for the same IP address(es):



As per above, the HTTP redirect rule will not be doing any authenticating:



All users should be allowed to hit http://example.com in order to be served the redirect response:



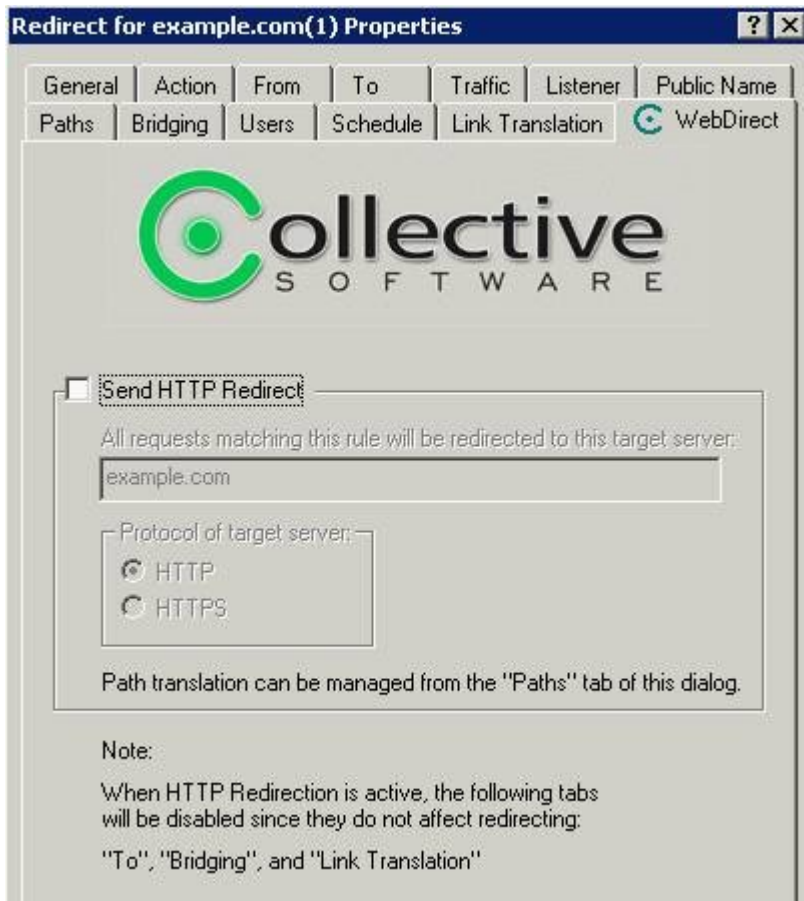
Now we have our redirector rule all set up. But at the moment, ISA thinks that there really is a server on your intranet that answers to the DNS name of “example.com”. This is where WebDirect comes in.

## Configuring WebDirect on the Redirector Rule

Select the properties item of the redirector rule we just configured above. If the WebDirect interface is installed, all web publishing rules should now contain a WebDirect tab:



On that tab we find options that control the redirect functionality:



For all publishing rules, the redirect feature is initially disabled. For our example to work, we will enable it, confirm the target host is "example.com", select HTTPS as the protocol. See below for the completed configuration:



Once the changes have been applied and the ISA servers synchronize to the new configuration (if you have Enterprise edition), then we are all done. Now any requests for `http://example.com/*` will receive an HTTP redirect response to the same URL, only in HTTPS.

## Advanced Path mapping

Here we will provide some more information about controlling the URL path that your redirects will use. If you are already familiar with the “Paths” tab of ISA Server 2004, then you can probably skip this section. WebDirect (starting with version 1.1) leverages the Paths tab for your Redirector rules, and the functionality is very similar to mapping paths on a normal publishing rule.

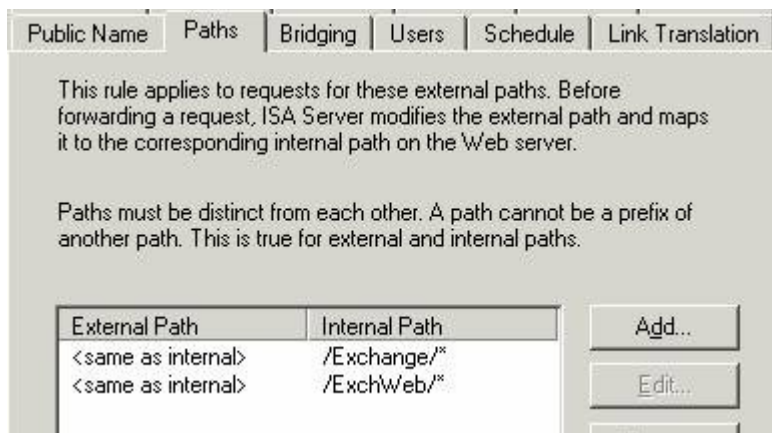
## OWA Redirection

If you need to route all incoming HTTP and HTTPS requests for the entire “example.com” server to “`https://example.com/Exchange`”, you would configure rules as follows:

Firewall Policy			
O...	Name	Action	Protocols
1	Real publishing rule for /Exchange/* on HTTPS	Allow	HTTPS
2	Redirect /* to /Exchange	Allow	HTTPS
3	Redirect HTTP to HTTPS	Allow	HTTP

The first rule should be your real Secure Publishing rule. Ideally you will have set up this rule with the Exchange publishing rule wizard. The paths below are only two of the ones that rule sets up. Leave your paths as they were configured by the wizard.

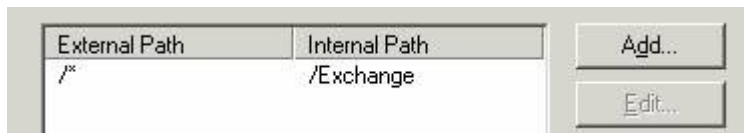




This rule needs to be first, because any requests for the Exchange folder on HTTPS don't need any redirection. (If we were to put the redirect first, then it would become a loop where requests would redirect through that rule forever!) Make sure you set up the paths correctly!

The second rule is the redirector that handles our path remapping. Follow the same steps as above for creating a **redirector rule**, except this time use the same **HTTPS listener** that you are using for rule 1 (i.e. make it a "Secure" publishing rule).

After you finish making the rule, go into the properties and look at the paths tab. We will be redirecting "example.com" to "example.com" with HTTPS on both sides. The Paths tab should be configured as:



Note that in this rule we say "/Exchange" and not "/Exchange/\*". This causes all HTTPS requests that don't hit the first rule to match here, and redirect to /Exchange (thus triggering rule 1 when the request comes back). This way we herd everyone who doesn't use "Exchange" onto the correct front page.

The third and final rule is the HTTP to HTTPS redirector. Set this up using the same steps as above for creating a **redirector rule**. No special path rules are needed.

End result: So if someone types in "http://example.com/foo" they first get redirected to "https://example.com/foo" by rule 3, then to "https://example.com/Exchange" by rule 2, then finally rule 1 serves the real request to the Exchange folder on your OWA server.

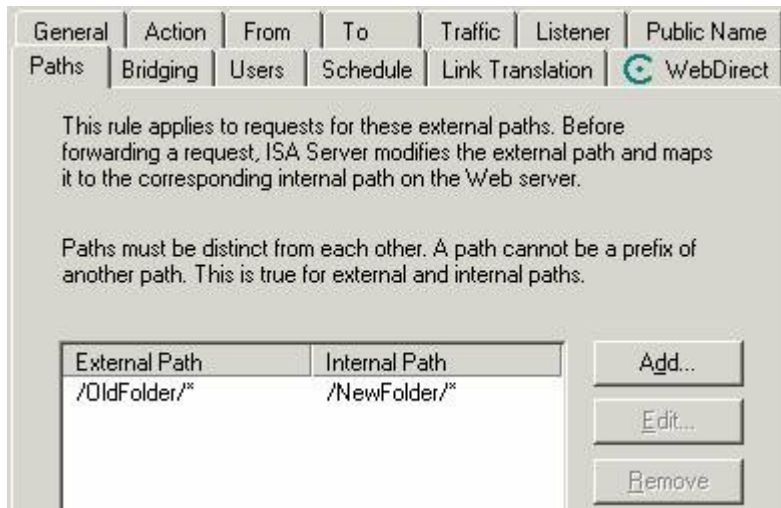
## "Folder Moved" Scenarios

In this case we begin with the exact scenario at the top of this document, but we have added a wrinkle. A folder on our web server has been renamed from "OldFolder" to "NewFolder". We don't want people with old URLs to encounter an error page, so here is how we will set up the rules:

O...	Name	Action	Protocols
1	Redirect OldFolder -> NewFolder	Allow	HTTPS
2	example.com	Allow	HTTPS
3	Redirect for example.com	Allow	HTTP

Rules 2 and 3 are exactly the way we set them up in the first part of this document, to publish the server and then redirect HTTP to HTTPS. But we insert a *new*, more specific rule *before* those. (If we put it below the real publishing rule then it would never redirect because the real publishing rule would always match first!)

Our rule 1 is a “Secure” publishing rule (must use the HTTPS listener). Set it up to redirect “example.com” to “example.com” with HTTPS on both sides. The Path tab is where we set up the real purpose of this rule:



Now any requests for “https://example.com/OldFolder/etc” will be redirected to “https://example.com/NewFolder/etc”.

End result: If someone types in “http://example.com/OldFolder/MyWord.doc” then rule 3 will redirect them to “https://example.com/OldFolder/MyWord.doc”. Rule 1 will send them to “https://example.com/NewFolder/MyWord.doc”. Finally, the real publishing rule (rule 2) will serve the word document that exists in the “NewFolder” folder on your web server.

## Path mapping without HTTPS

If your redirect scenarios don’t call for HTTP to HTTPS redirects, you can follow the previous example with the following changes:

- Rule 1 will use the normal HTTP listener (create it as a normal Web Publishing rule, then convert it to a Redirect in the WebDirect tab).
- Rule 3 is not needed.

## **General path mapping rules**

The examples shown here are just to illustrate common usage scenarios. You can use publishing rules, secure publishing rules, and WebDirect redirection capabilities to solve almost any path mapping problems. Just keep in mind to put your path-specific rules *higher* in the ordering than the path-neutral “/\*” rules. If you put the general rules first, then they will *always* match, and your path-specific rules won't ever get a chance to work!

## **Additional assistance**

If you are having trouble making WebDirect fit the redirection needs of your organization, please contact [our support staff](#), and we will do our best to help!