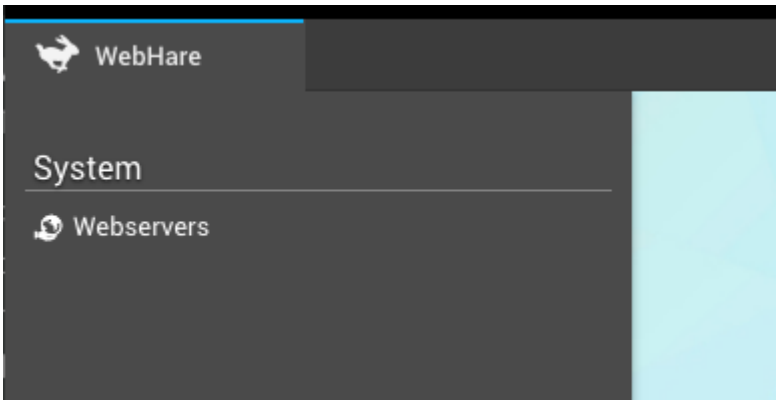
Webservers

You can set up Webservers using the Webservers application. The application is listed under the "System" group of the WebHare menu:



The button bar contains the most often used actions. All actions can also be found in the menu on the far right of the button bar:

The main screen offers an overview of existing webservers. Three types of server are supported:

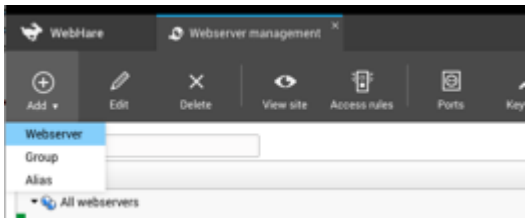
- WebHare backend interface server: usually one of these is configured. This webserver provides the webserver for the WebHare interface, allowing users to log on and run applications
- WebHare output server. This webserver type provides an output webserver, usually to publish a website.
- Access rules only - no published content. This can be used for redirecting visitors to another location.

Every severtype supports aliases. There are two types of aliases:

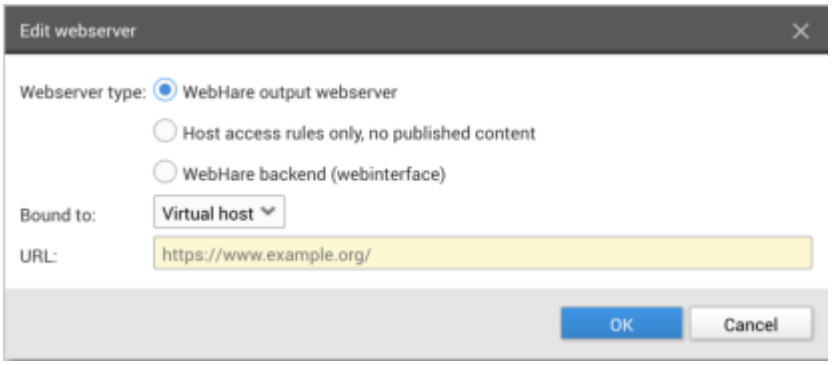
- Alternative hostname: the address will not be changed when the visitor uses this.
- Redirect: the visitor will be redirected to the main hostname.

Adding a webserver

1. Click the "Add" button and choose "Webserver".

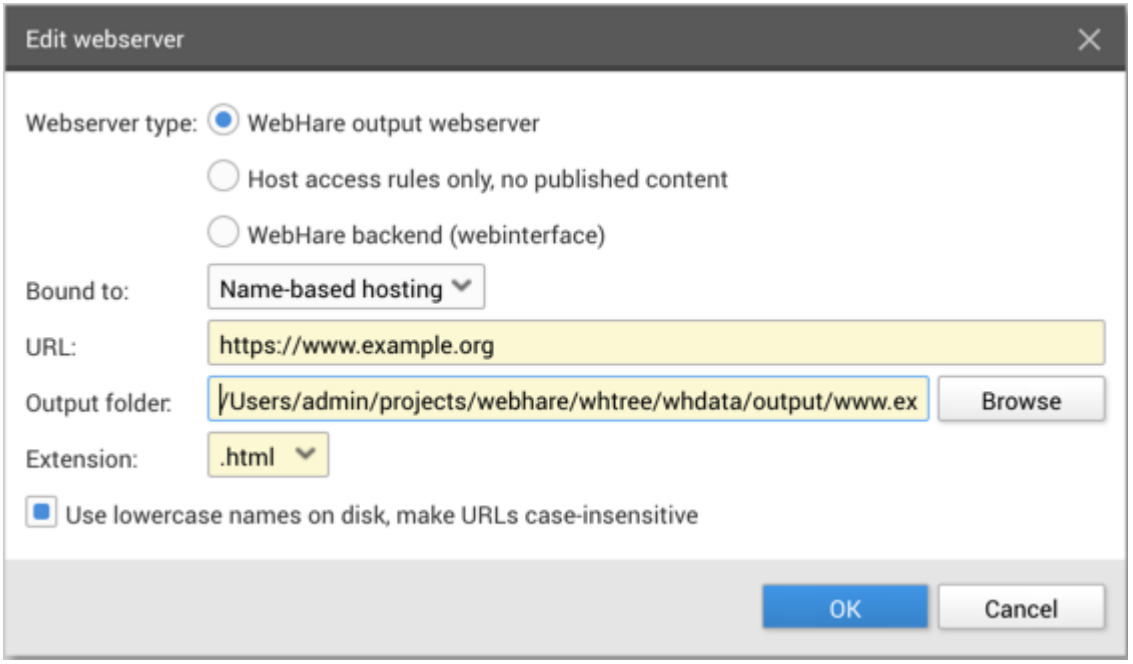


2. The "Edit webserver" screen is opened.
3. Choose the appropriate settings for your goal:



4. Choose the desired webserver type (see the descriptions above).
5. Choose the binding type; usually this is "Virtual host" (or name based), where the URL domain name is used to look up the corresponding webserver.
6. Choose the URL.
7. Click "OK" to save the webserver.

An output folder is automatically choosen. You can change this by editing the created webserver:



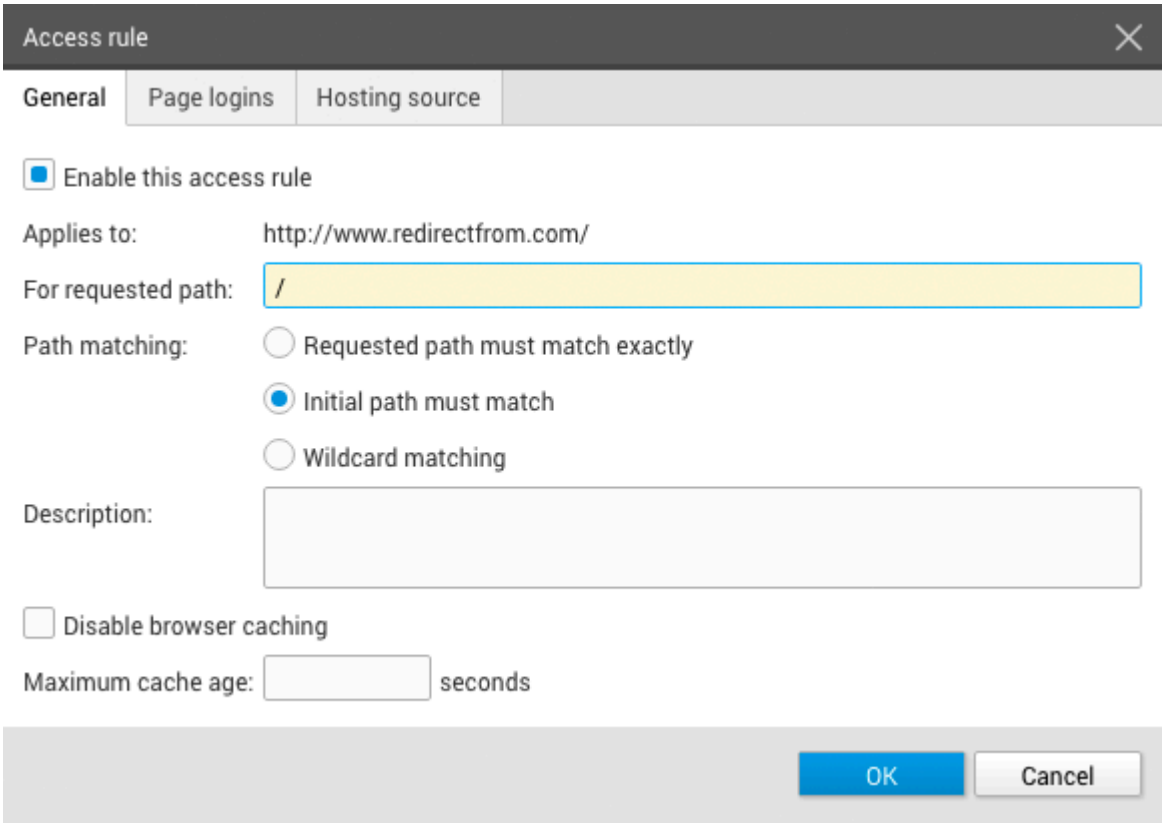
Access rules

Access rules are used to set rules for (part of) a webserver for (part of) the visitors. You can redirect users based on IP rules or (WebHare or other) login.

To set one or more access rules for a webserver:

- Select the webserver you have created.
- Choose "Access rules" from the button bar.

Choose "Add" to add an access rule. Several settings are available, divided over 3 tabs.



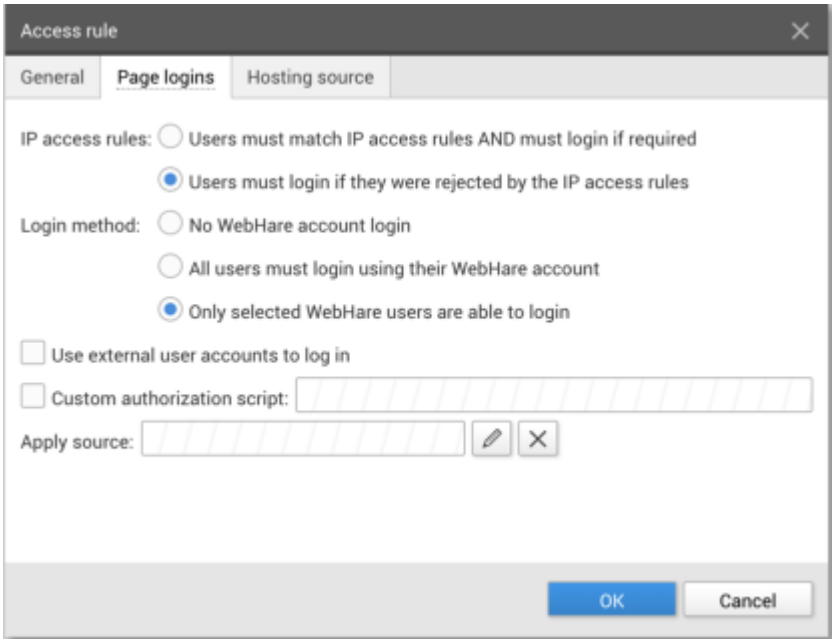
The "General" tab houses the following settings:

- Enabling / disabling the access rule.
- Choose which path you want: when you add "/" or nothing the webserver root is used, when you add "/folder/" the rule is applied to the subfolder "folder".
- "Path matching" defines what happens next:
  - Exact match: only the requested path is used, for any other path the rule is not applied
  - Initial path must match: the rule is applied for everything after the path. In the "/folder/" example on "folder/subfolder" the rule is applied.
  - Wildcard matching allows for setting up advanced rules. "*/images/" for instances would be applied to all folders named "images" within any part of the webserver.
- You can choose to disable browser caching or limit the cache age.

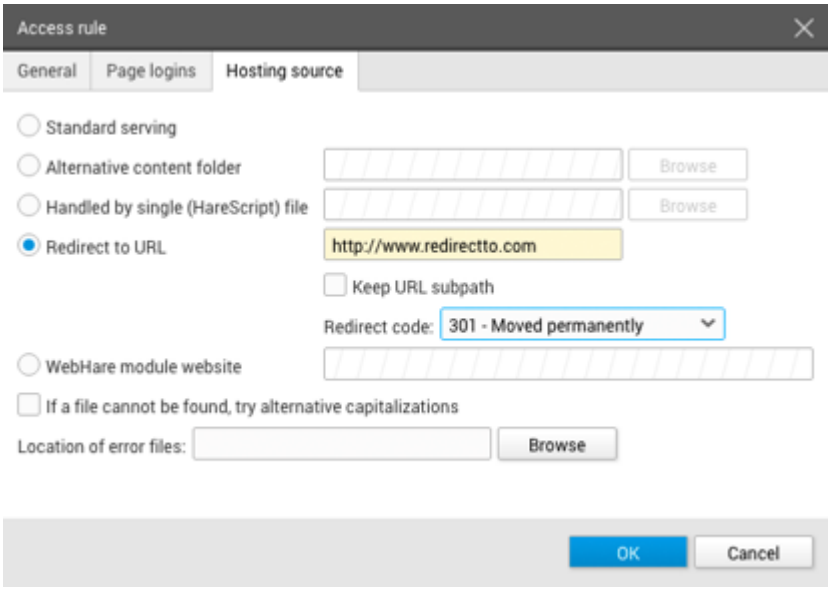
The "Page logins" tabs lets you choose in which way visitors to the website are identified:

- Based on IP rules - these need to be set separately (see Setting IP-filters). You can choose whether only users that don't meet the IP filters need to login or only users that don't meet the IP filters.

- Login method: you can set rules based on WebHare accounts - either all WebHare users available in User Management or selected users. You can choose these WebHare users separately (see choosing WebHare users).
- External user accounts; you can create "External user accounts" for loggin on (See "External users". These will then be able to login to the website, but not the application backend.



The "Hosting source" tab allows you to choose what hosting choices are made based on the set access rule.



- Standard serving: usually used in combination with login settings to restrict visitors

- Alternative content folder: can be used to show different content do different visitor groups.
- Single script: allow a single script to handle all visitors
- Redirect: redirect to a different URL.

- You van choose to keep the URL subpath.

- A WebHare module website can also be used as hosting source.

Setting IP filters

- Open the access rules dialog.
- Select an access rule and press "IP filters".
- An overview of current filters is displayed.
- Choose "Add" to add a new filter.
- Add the relevant IP mask. CIDR notation are supported.
- Choose whether this IP filter denies or allows access. When access is allowed based on this filter, all other IP's are denied (and vice versa), except for IP's set by other filters.

Choosing WebHare users for access

- Open the acces rules dialog.
- Select an access rule where "Only selected WebHare users" is selected for login method
- Click the "WebHare users" button.

The users that have access are displayed.

- Click "Grant right" you add users that can login.
- Choose the user(s) you want to allow to login.

Setting External Users

- Open the acces rules dialog.
- Select an access rule where "Use external user accounts to login " is selected.
- Click the "External users" button.

The users that have access are displayed.

- Click "Add" you add users that can login.
- Enter a username.
- Enter a (secure) password.
- Repeat the password.
- Click "OK" to add the user.

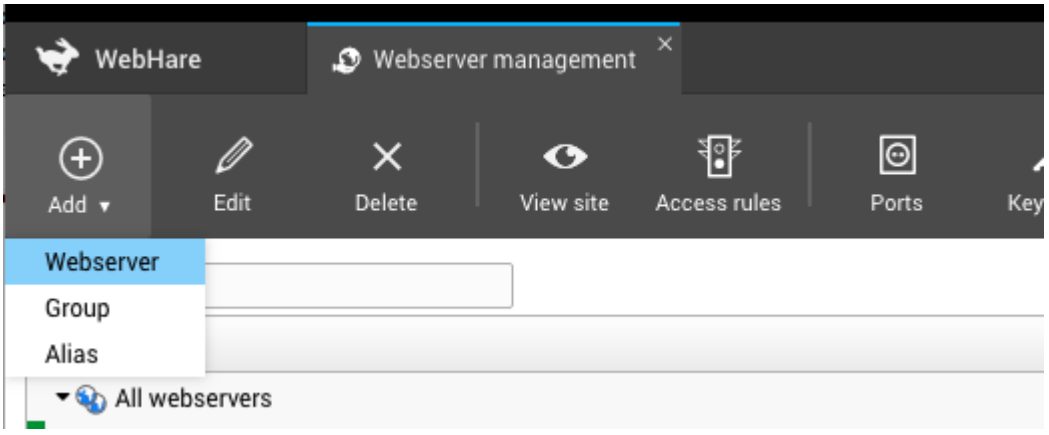
Provide the user with the username and password to provide access.

Redirect

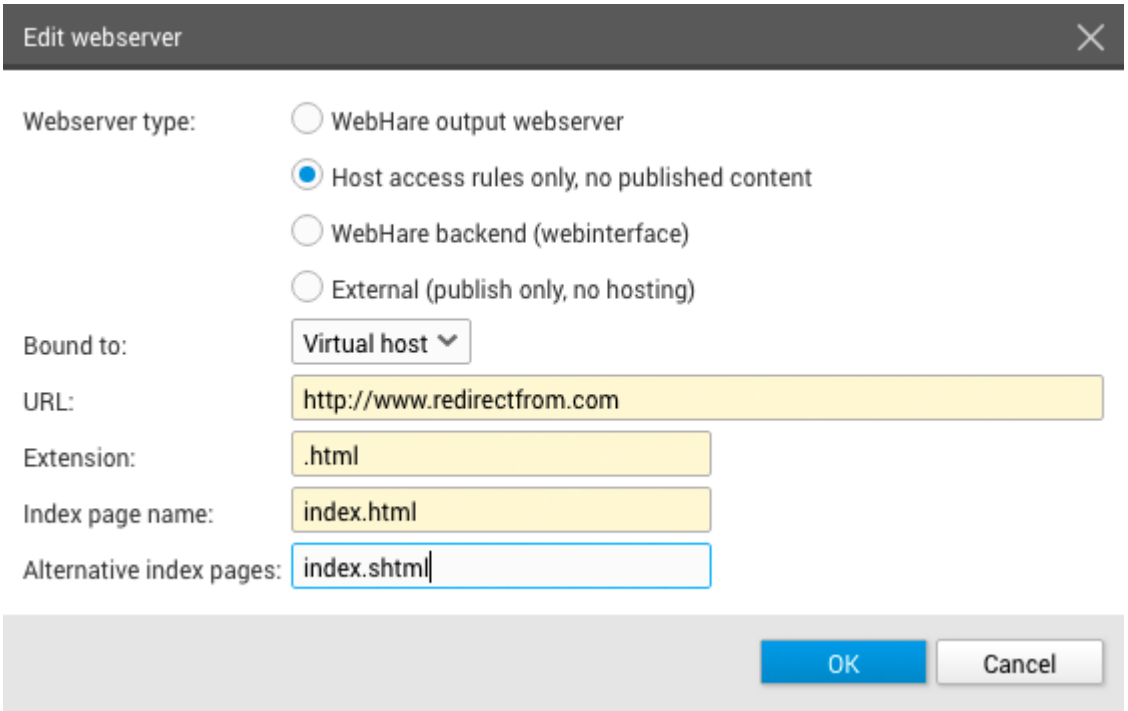
To create a website redirect you need to create or choose a webserver, configure the webserver and add the appropriate access rule.

Adding a webserver

After starting the application you can add a webserver by clicking the "Add" button and choosing "Webserver".



The following settings are needed for a redirect-only webserver:



Where *http://www.redirectfrom.com* is the domain you want to redirect visitors from.

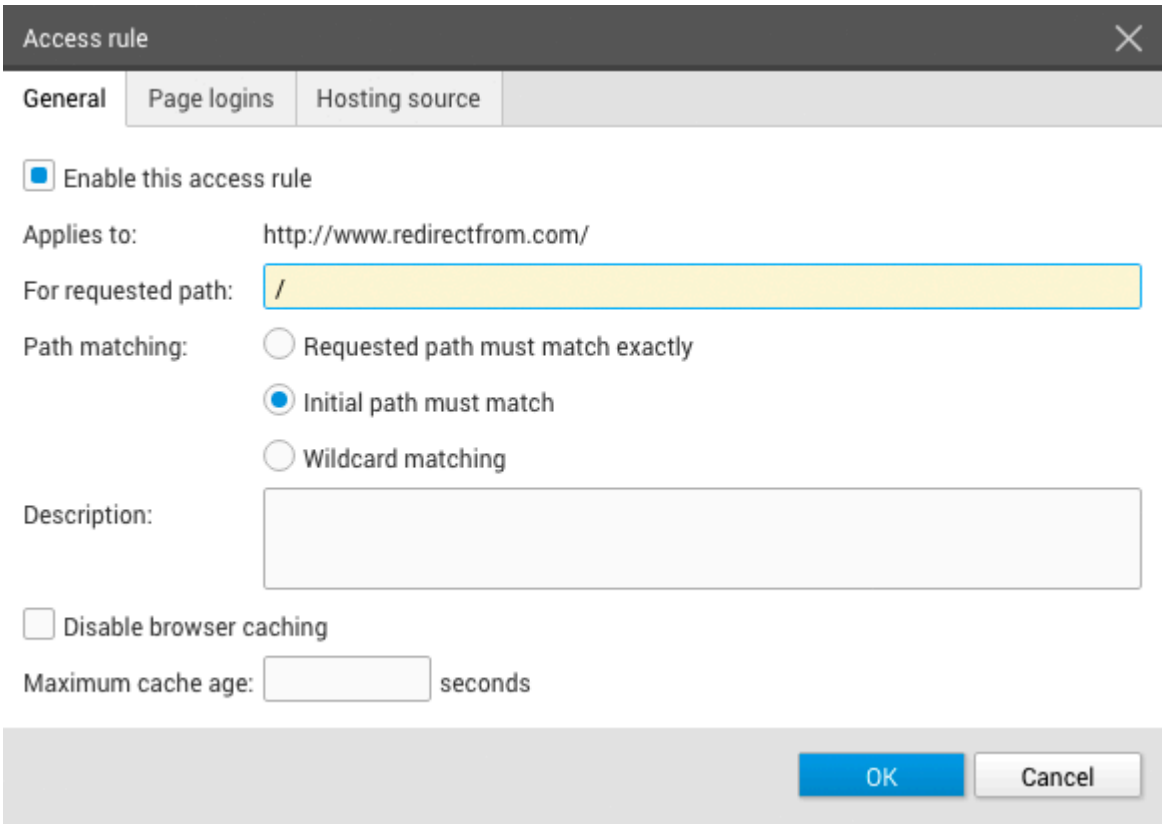
Click "OK" to save the webserver.

The webserver has been added, but the redirect needs to be set through *access rules*.

Setting access rules

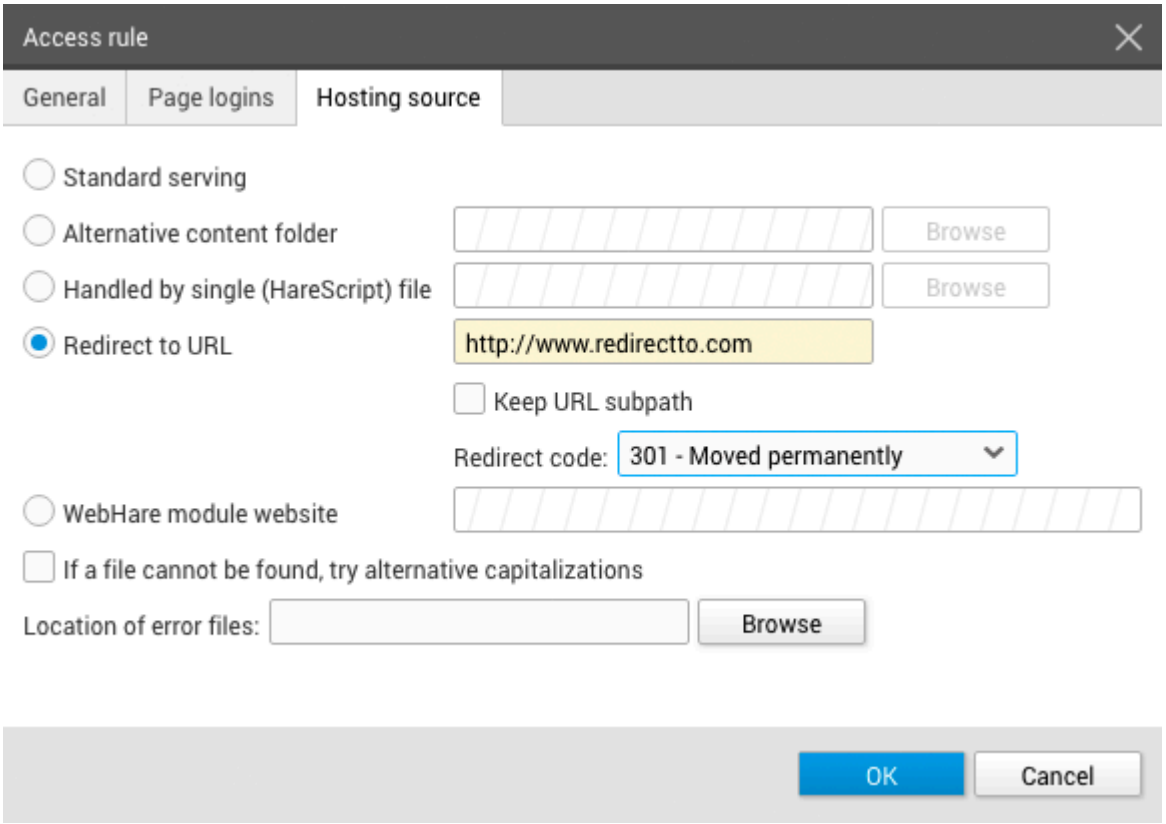
- Select the webserver you have created.
- Choose "Access rules" from the button bar.

- Choose "Add"



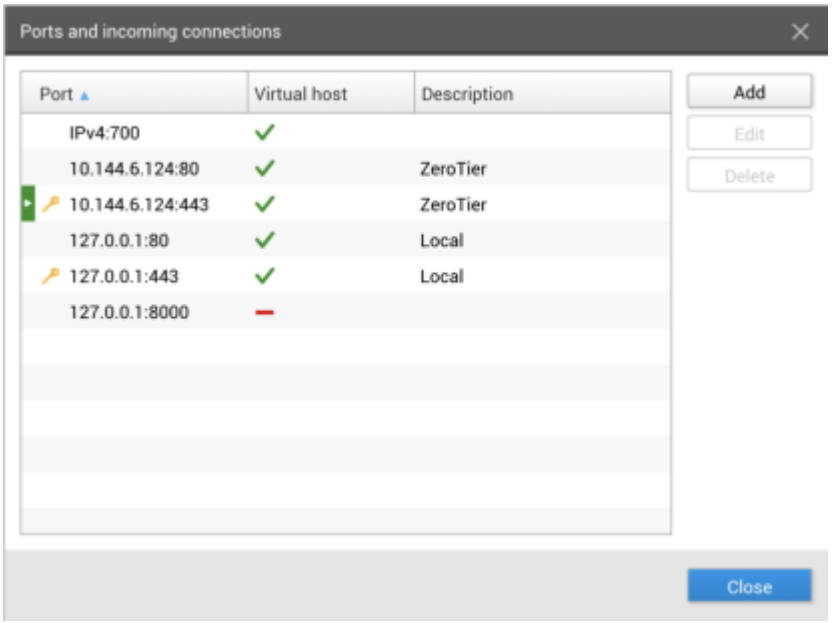
- Make sure the access rule is enabled.
- Set the request path to /
- Set "Path matching" to "Initial path must match".

- Open the "Hosting source" tab

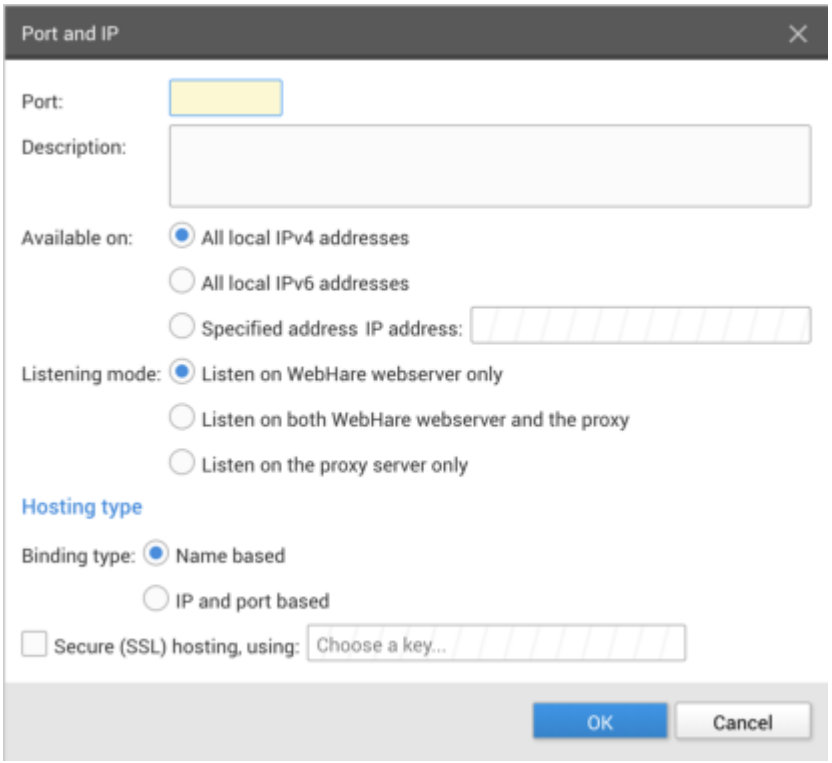


- Choose "redirect to URL" and choose the desired redirect code.
- Click OK to add the access rule.
- Click OK again to save the access rules for the webserver.

You can set the port and incoming connections from the button bar.

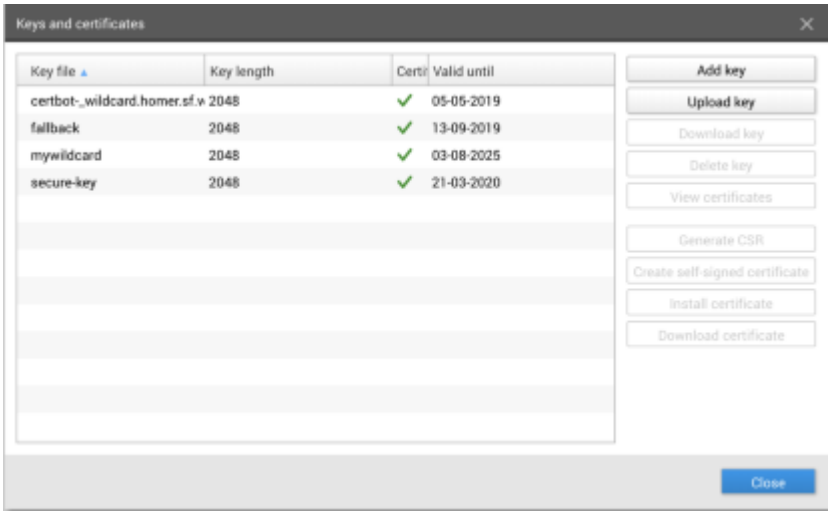


For website hosting, usually ports 80 and 443 are configured to handle name based port bindings.



To add a binding for port and IP, fill in the port field and set the other settings.

- In most cases name based binding is used, allthough IP and port based can be used for a backend server.
- To enable SSL hosting, you must first set up a key.



LetsEncrypt certificates

WebHare can use free and automated certificates from LetsEncrypt. These certificate requests are verified using the HTTP-01 challenge which has the following requirements before you can request a certificate:

- The WebHare creating the certificate needs to respond to requests for the insecure (http) version of the website.
- Port 80 needs to be reachable from the internet (and remain available for automatic renewal).

You should verify you can reach the website over port 80 before requesting a certificate - trying to request a certificate if the DNS isn't working yet may slow down later requests (as you need to wait for LetsEncrypt's cached DNS entries to expire)

The initial request of a LetsEncrypt certificate can only be done on the WebHare command line:

```
wh ssl certbot <primary domain name> [altname] [altname...]
```

The certificates will be renewed when it has less than 30 days of validity left. If this fails, WebHare will retry daily and start warning when the certificate has less than 21 days of validity left.

Migrating certificates

If you need to migrate an existing HTTPS website not currently hosted on your server, you may not be able to use LetsEncrypt for the initial certificate as you can't yet have WebHare respond to the challenge. In this case it's often best to ask the current site owner for their private key and certificate and upload these to WebHare. If that's not an option you could consider buying a certficate from a certificate provider that does a different type of validation.

We recommended against disabling HTTPS or use self signed certificates during migration as that may make the site temporarily unavailable during the migration, especially if the site to migrate is using Strict Transport Security.