Purpose

This document describes how use the Website Defacement Wizard to monitor your websites for defacement, modification and malicious insertions with Nagios XI. The Website Defacement Wizard provides an automated method for monitoring your website for defacement, and notifies you when your website contains undesirable content.

Target Audience

This document is intended for use by Nagios XI Administrators and end-users who want to monitor their websites for defacement.

Considerations

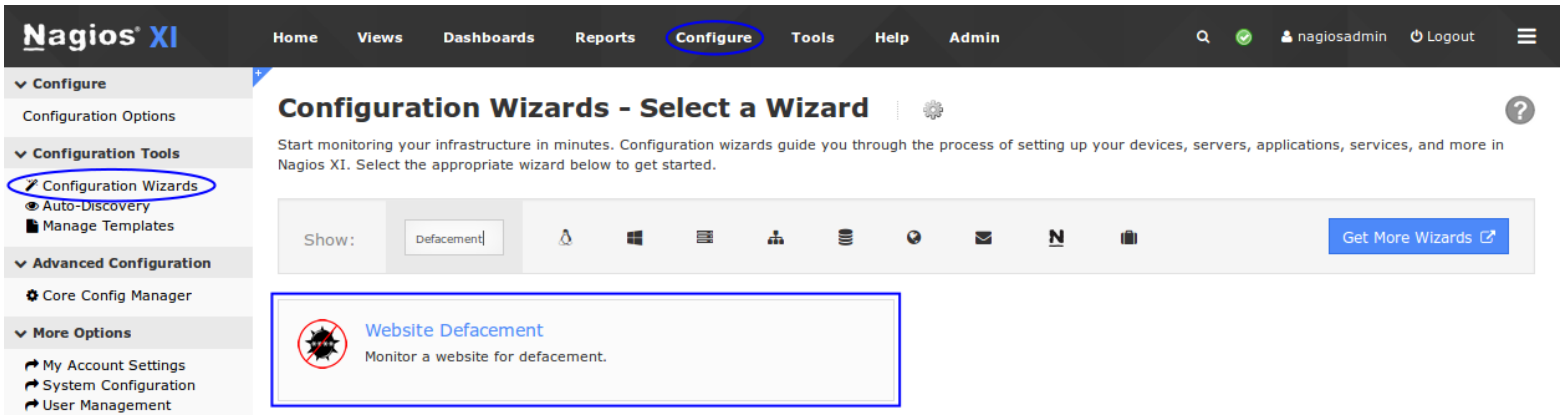
When monitoring a website for defacement, consider the following:

- The Website Defacement wizard uses a regular expression check to search for a specific string or multiple strings
- Strings do not have to be case sensitive and each one should be separated by a new line
- There are a few pre-defined lists of words you may want to search for, sorted into categories
- You can also load a custom wordlist file into the wizard for each site you want to monitor
- There is also a regular expression match check to verify that the website you are monitoring is up and running, but this is strictly optional and may be redundant if you are already monitoring this website with Nagios XI

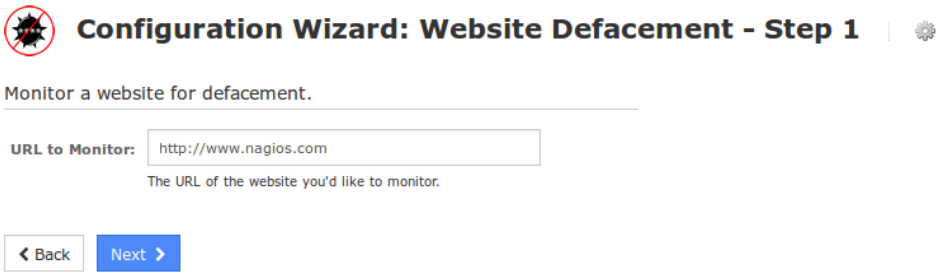
The Website Defacement Wizard

This Website Defacement wizard uses the regular expression check to find a specific string that you do not want to appear on your website. You receive a critical response when the check finds one or more of the strings it was instructed to search for on the website. To understand the capabilities of the wizard we will walk through an example.

To begin using the Website Defacement wizard navigate via the top menu bar to **Configure** > **Run a configuration** wizard, and select the **Website Defacement** wizard. In the following screenshot you can see how the search field allows you to quickly find a wizard.



In Step 1, enter the **URL** of the website you want to monitor into the **URL to Monitor** field.



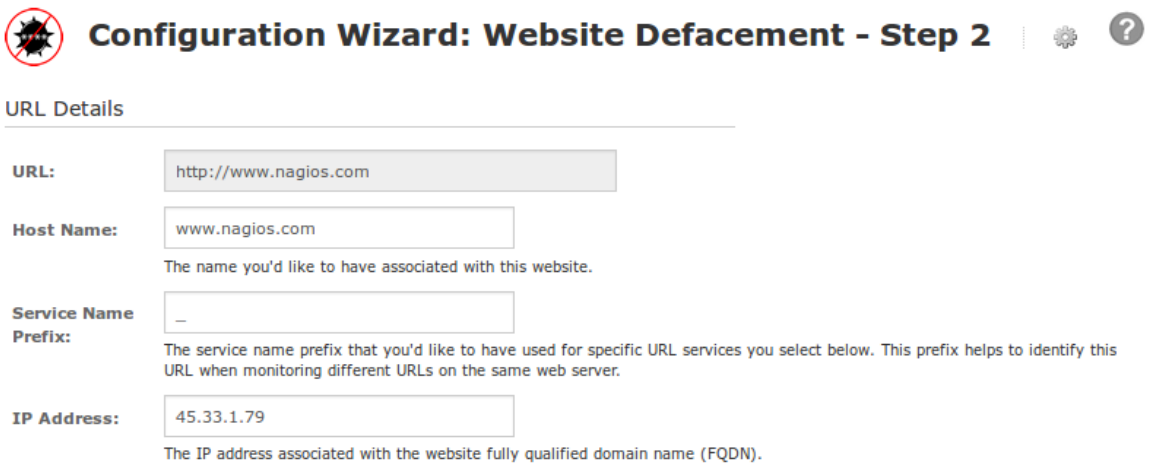
This can be the main page of the website or any specific sub-page you want to monitor. Click Next to proceed to Step 2.

Step 2 is where the majority of the configuration takes place and is broken up into multiple sections.

URL Details specifies the following:

- **Host Name** is the standard Nagios host name
- **Service Name Prefix** is a string that will be added to the beginning of any services created by the wizard for easier identification
- **IP Address** allows you to specify a different IP from the one that was auto-detected for the URL

Please refer to the screenshot on the following page.



URL Options specifies the following:

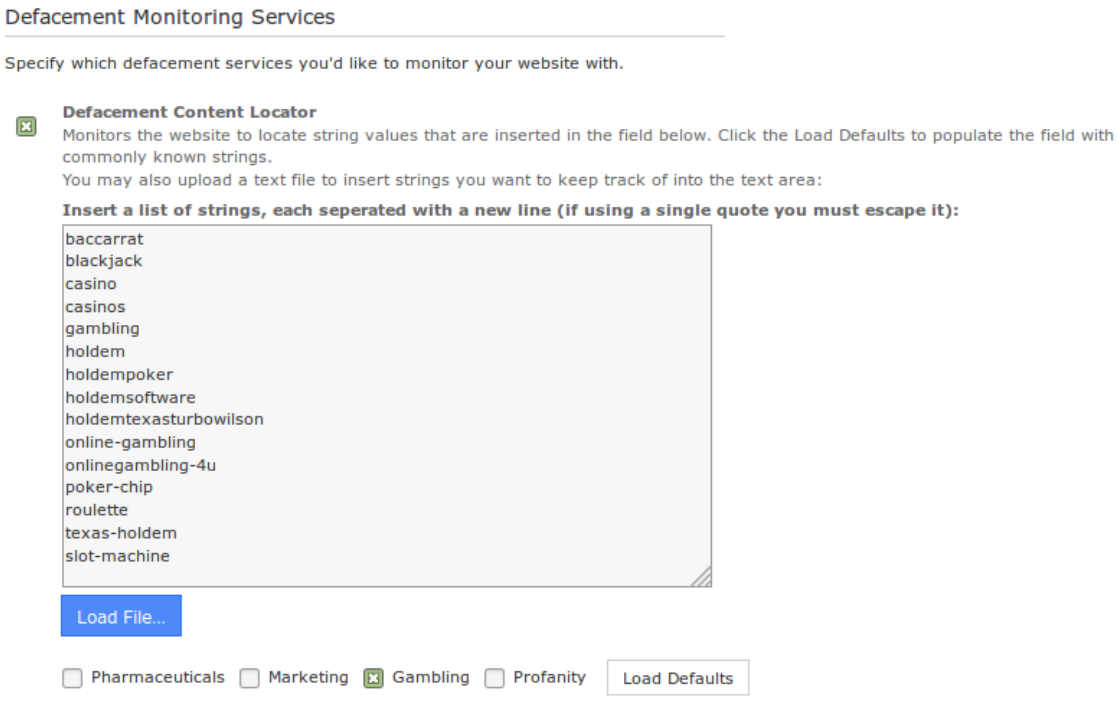
- **Use SSL** and **Port** can be configured in case HTTP/S are running on alternative ports
- **On Redirect** allows you to define how to handle redirected pages.
- **Credentials** allow you to specify a username and password for use in basic HTTP authentication

Defacement Monitoring Services allows you to select which defacement methods you would like to use to monitor your website. If you check the box next to **Defacement Content Locator** then a **Website Defacement** service will be created.

The **Defacement Content Locator** allows you to enter a list of words which should be considered "bad" if they appear on the page.

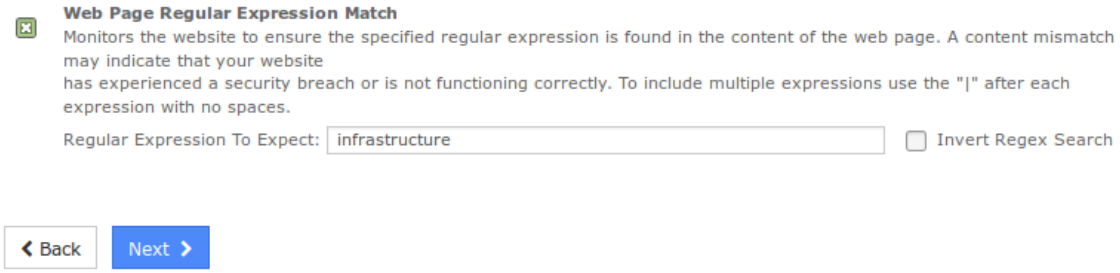
- You can enter in a list of words manually, one on each line
- You can upload a custom text file of words, also one on each line
- You can choose from the pre-defined lists of default words from different categories

From the screenshot below you can see that the **Gambling** checkbox was selected and the **Load Defaults** button was clicked. This loaded all the gambling related words to the text area input.



Web Page Regular Expression Match allows you to check that the content of the webpage includes specific words or expressions. If you check the box next to **Web Page Regular Expression Match** then a **Web Page Regex Match** service will be created.

You will then enter a string you wish to search for on the website. You will be alerted if the entered string does **not** appear on your website. You can also choose to invert the search by checking the **Invert Regex Search** check box. This will instead alert if the regex **is** found on your website.



Once you've finished making your selections, click Next and then complete the wizard by choosing the required options in Step 3 – Step 5.

To finish up, click on **Finish** in the final step of the wizard, this will create the new hosts and services and begin monitoring.

Once the wizard applies the configuration, click the **View status details for *your web server*** link to see the new host and services that were created.

Host	Service	Status	Duration	Attempt	Last Check	Status Information
www.nagios.com	_ Web Page Regex Match	Critical	1m 29s	2/5	2016-12-07 11:33:31	HTTP CRITICAL: HTTP/1.1 301 Moved Permanently - pattern not found - 461 bytes in 0.582 second response time
	_ Website Defacement	Ok	7s	1/5	2016-12-07 11:33:55	HTTP OK: HTTP/1.1 301 Moved Permanently - 461 bytes in 0.525 second response time

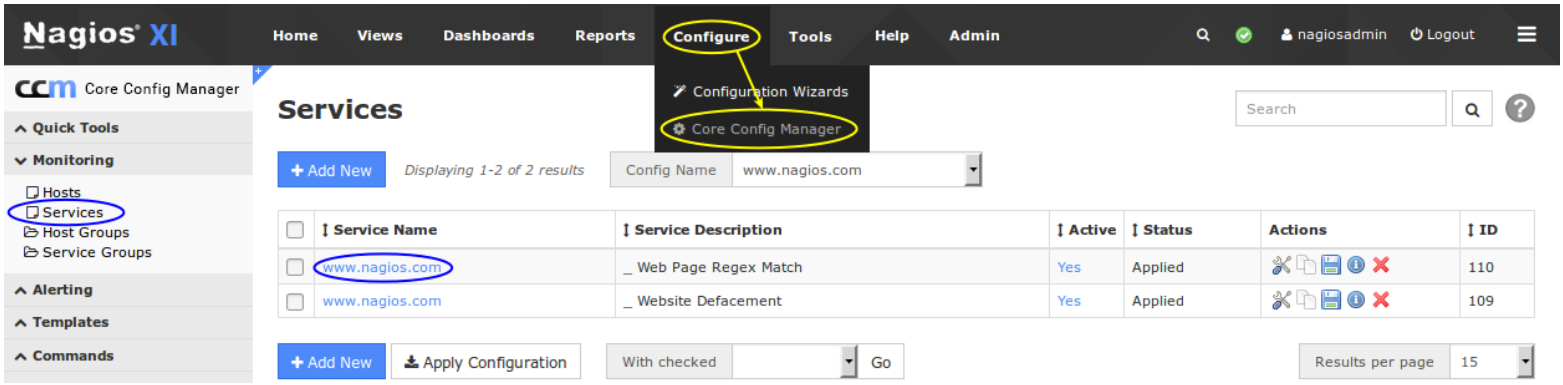
In the screenshot on the previous page you can see that the **Web Page Regex Service** is in a critical state with the error `"301 Moved Permanently - pattern not found"`. This will be resolved in the following troubleshooting section.

It's also worth mentioning that while the **Website Defacement Service** is in an OK state, it is also is reporting `"301 Moved Permanently - pattern not found"` and will need to be corrected for the service to function properly.

Troubleshooting

Some sites will issue a `HTTP 301` code which is just a simple redirect and can cause some issues with the `check_http` plugin (as seen in the previous screenshot). You will need to adjust the `"-f xxxx"` switch on the services to use the **`follow`** argument.

Locate the services by navigating to **Configure** > **Core Config Manager** > **Monitoring** > **Services.**

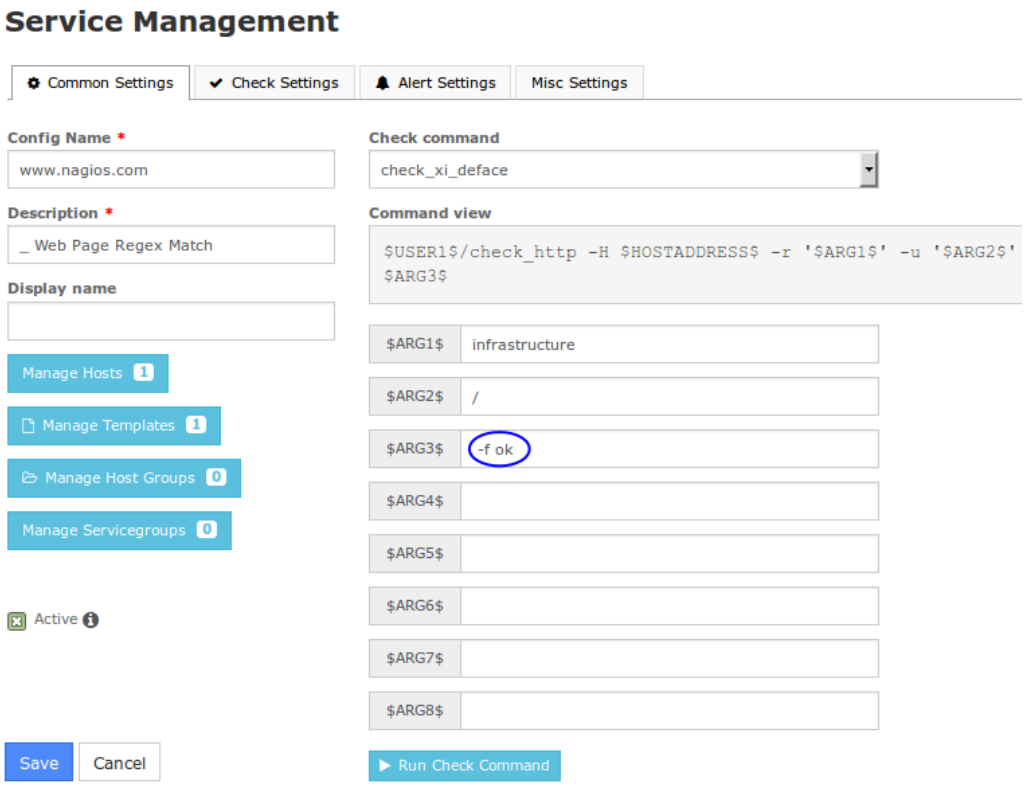


Click of the services in the **Service Name** column to begin **editing** it.

In the screenshot to the right you can see that **$ARG3$** has the value:

```
-f ok
```

Change **ok** to **follow**.

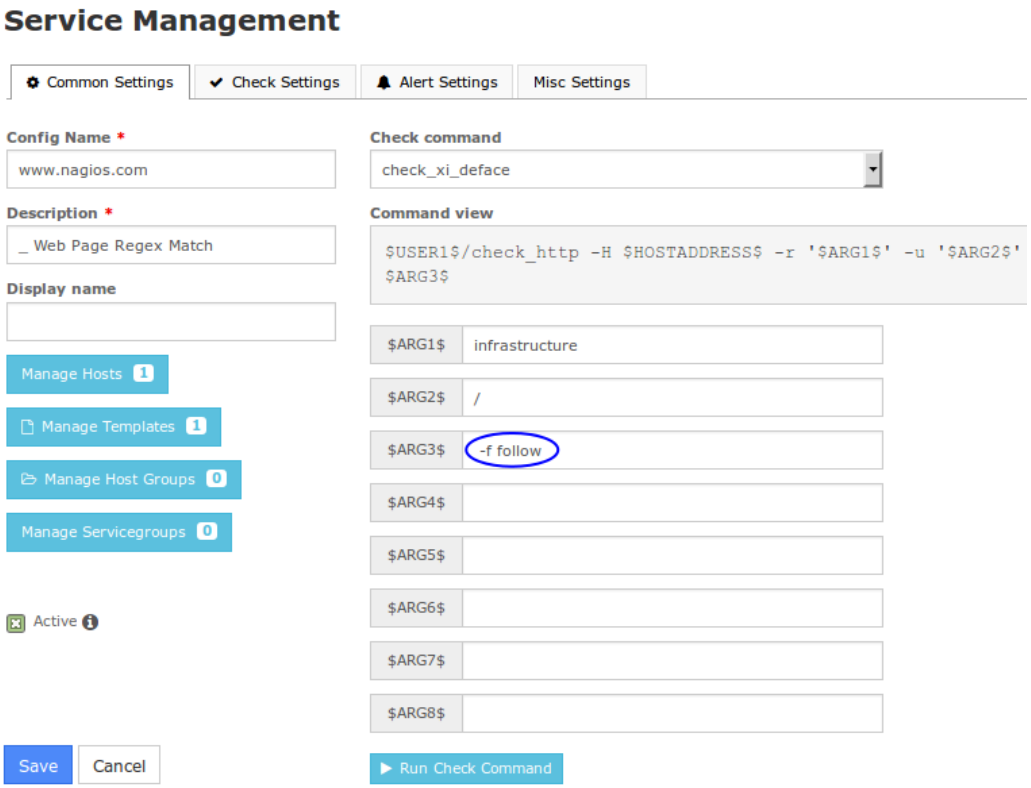


In the screenshot to the right you can see that **$ARG3$** now has the value:

```
-f follow
```

Click **Save** to save the changes.

Repeat this for any other services than need updating and then click **Apply Configuration** to make the changes go into production.



Once the configuration has applied go and view the services. After they've performed a check with the new setting they should be working correctly.

Host	Service	Status	Duration	Attempt	Last Check	Status Information
www.nagios.com	_ Web Page Regex Match	Ok	3h 17m 8s	1/5	2016-12-07 14:51:15	HTTP OK: HTTP/1.1 200 OK - 57419 bytes in 2.606 second response time
	_ Website Defacement	Ok	3h 19m 36s	1/5	2016-12-07 14:53:20	HTTP OK: HTTP/1.1 200 OK - 57431 bytes in 2.581 second response time

Finishing Up

This completes the documentation on how to monitor website defacement in Nagios XI.

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

https://support.nagios.com/kb