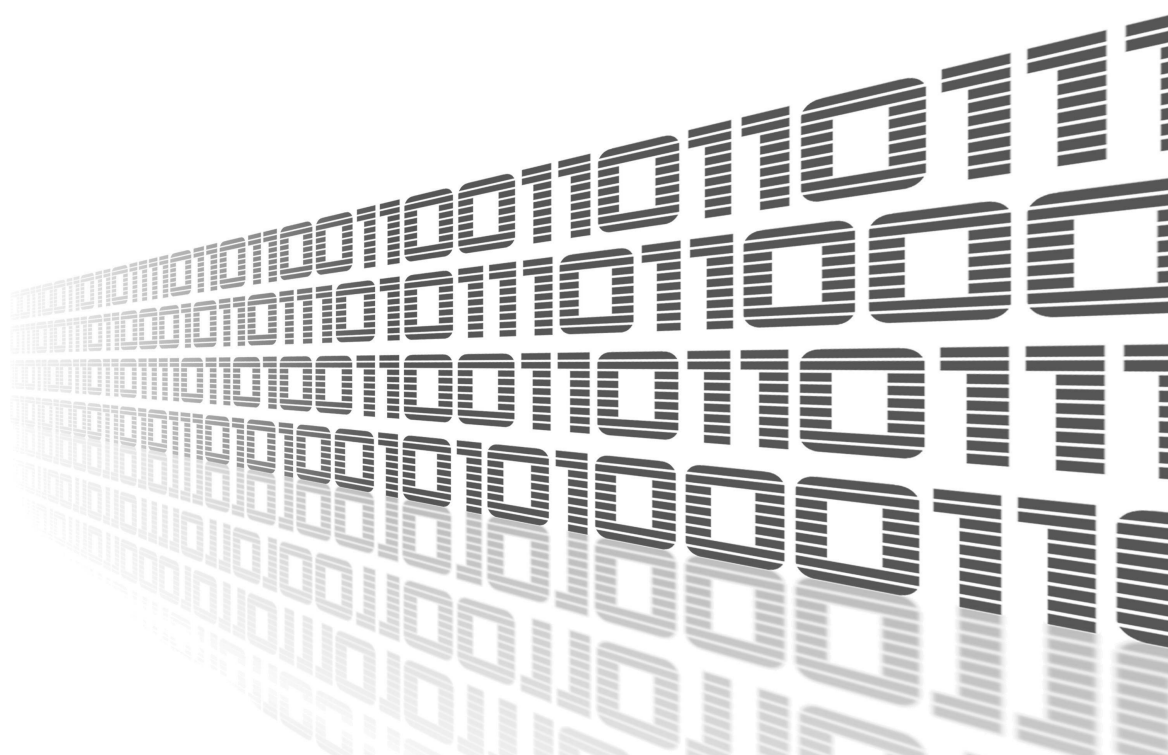




User Module

# URL Blocker

APPLICATION NOTE



## Used symbols



*Danger* – Information regarding user safety or potential damage to the router.



*Attention* – Problems that may arise in specific situations.



*Information or notice* – Useful tips or information of special interest.



*Example* – example of function, command or script.



Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic  
Document No. APP-0016-EN, revised on June 18, 2020. Released in the Czech Republic.

# Contents

<b>1</b>	<b>User Module Description</b>	<b>1</b>
<b>2</b>	<b>Configuration of URL Blocker</b>	<b>2</b>
<b>3</b>	<b>Related Documents</b>	<b>5</b>

## List of Figures

1	Router with <i>URL Blocker</i> user module installed . . . . .	1
2	<i>URL Blocker</i> menu . . . . .	1
3	Disabled URL blocking . . . . .	2
4	Example of blocking enabled . . . . .	2
5	Enabled URL blocking . . . . .	3
6	Example of redirecting mode . . . . .	3
7	Default information page after redirection . . . . .	4
8	Upload custom welcome/banned page form . . . . .	4
9	Successful upload of custom welcome/banned page . . . . .	4

# 1. User Module Description

*URL Blocker* user module enables blocking of certain domain names (URLs) so the users connected to the Advantech router cannot access them. Blocking is based on iptables rules (*Blocking* mode) or intentionally forged DNS records sent from Advantech router to connected users (*Redirecting* mode). There are 16 fields in configuration form so it is possible to block up to 16 different domains with the *URL Blocker* user module. Note that blocking does not work when the traffic is in encrypted tunnel (domain name cannot be read from packets).

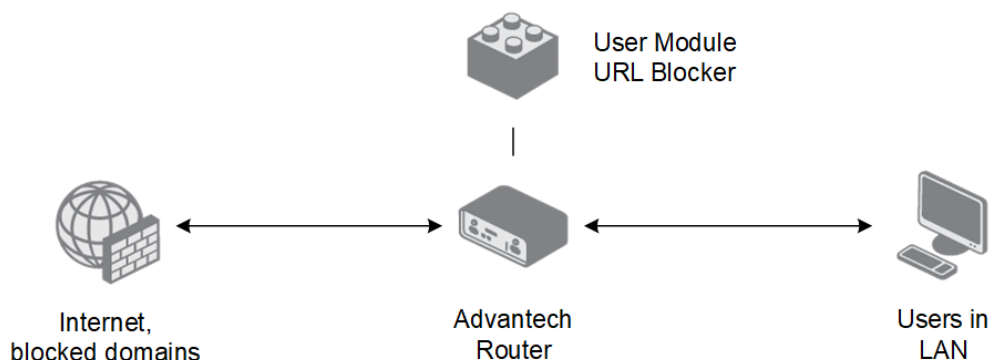


Figure 1: Router with *URL Blocker* user module installed



The *URL Blocker* user module is not part of the router's firmware. It can be downloaded from <https://ep.advantech-bb.cz/user-modules>. The installation process for the user modules is described in the Configuration Manual (see [1, 2, 3 or 4]). The user module is compatible with v2 and v3 routers.

## URL Blocker

Status
Global
Configuration
URL Blocker
Welcome/Banned Page
Customization
Return

The Web interface of the user module is accessible by clicking on the user module's name on the *User Modules* page in the router. On the left there is user module's menu as in Figure 2. There is *Global* landing page in the *Status* section. In the *Configuration* section there is *URL Blocker* page with configuration followed by *Welcome/Banned Page* where custom destination page for redirect mode can be uploaded. You can return to the Web interface of the router using *Return* button in the *Customization* section.

Figure 2: *URL Blocker* menu

## 2. Configuration of URL Blocker

After installation, the *Global* page in *Status* section shows this information:



Figure 3: Disabled URL blocking

To enable blocking, go to *URL Blocker* page in *Configuration* section and check the *Enable URL Blocking* checkbox. Two modes of behaviour are possible: 1) **Blocking**, where the blocked page shows just browser DNS error, or 2) **Redirecting**, where the custom blocked page information is shown to the user. Choose *Blocking* option in the select field, fill in the intended domains you want to block and click the *Apply* button.

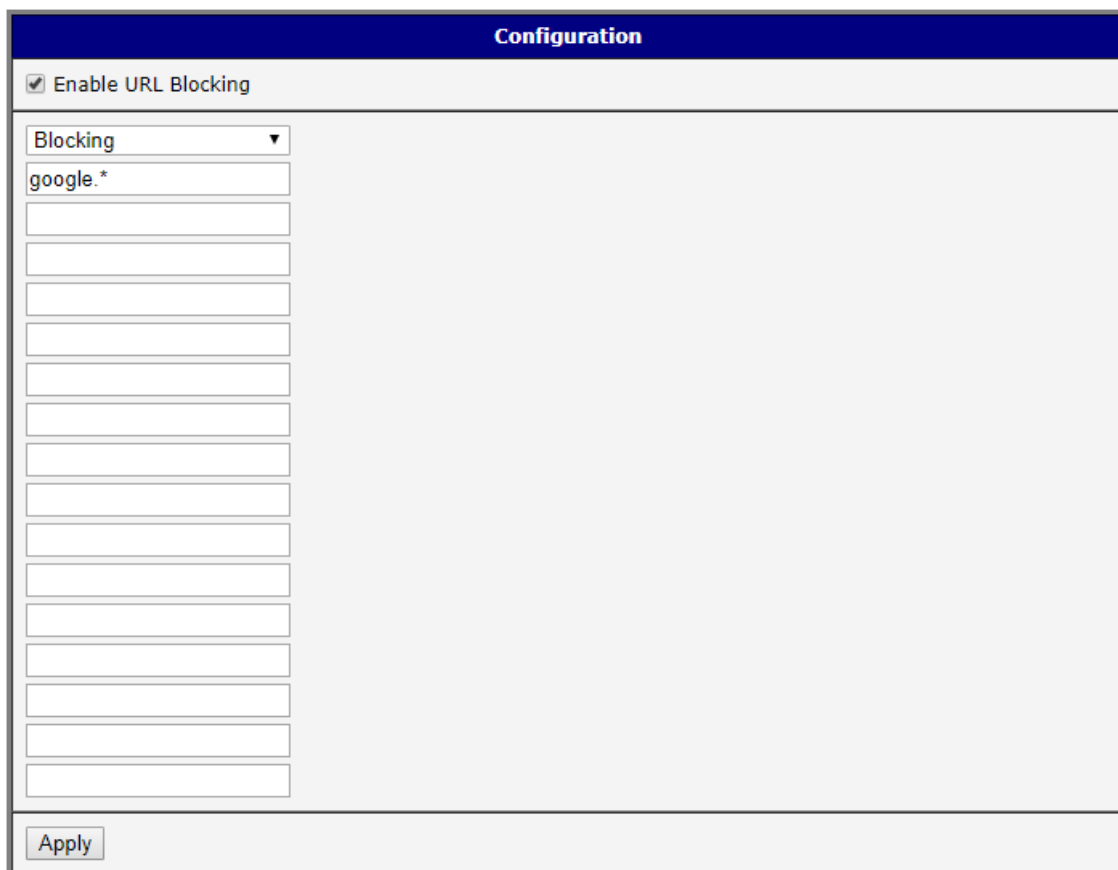
A screenshot of the 'Configuration' page for the URL Blocker. The page has a dark blue header with the text 'Configuration' in white. Below the header, there is a checkbox labeled 'Enable URL Blocking' which is checked. Underneath the checkbox is a dropdown menu currently set to 'Blocking'. Below the dropdown is a list of text input fields for domains; the first field contains 'google.\*' and the others are empty. At the bottom of the form is an 'Apply' button.

Figure 4: Example of blocking enabled

Now there is enabled information showing on the *Global* page in the *Status* section:

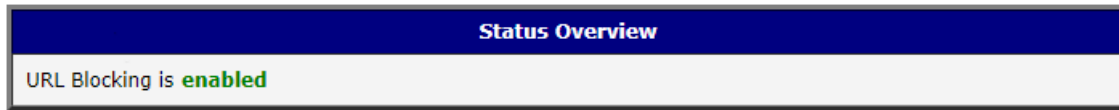


Figure 5: Enabled URL blocking



In *Blocking* mode you can use asterisk \* character as a substitute for top level domain. You can see this in Figure 4. All top level domains with the same domain name are then blocked. The substitute \* character does not work in the *Redirecting* mode. The redirection works in HTTP only. In HTTPS, the blocking is used instead (Welcome/Banned page does not appear). All subdomains (www., mail., etc.) of the listed domains are blocked by default in both modes.

Note: when testing the user module configuration, do not forget to clear cache of the browser or restart it. Most of Web browsers cache DNS records for themselves.

There is an example of *Redirecting* mode in the next Figure.

A screenshot of the 'Configuration' page. The title 'Configuration' is in a dark blue header. Below the header, there is a checkbox labeled 'Enable URL Blocking' which is checked. Underneath, there is a dropdown menu currently set to 'Redirecting'. Below the dropdown is a list of text input fields for domain names; the first field contains 'google.com' and the others are empty. At the bottom left of the configuration area is an 'Apply' button.

Figure 6: Example of redirecting mode

In this mode the default Welcome/Banned page will tell the user the page is blocked as you can see in the Figure below:

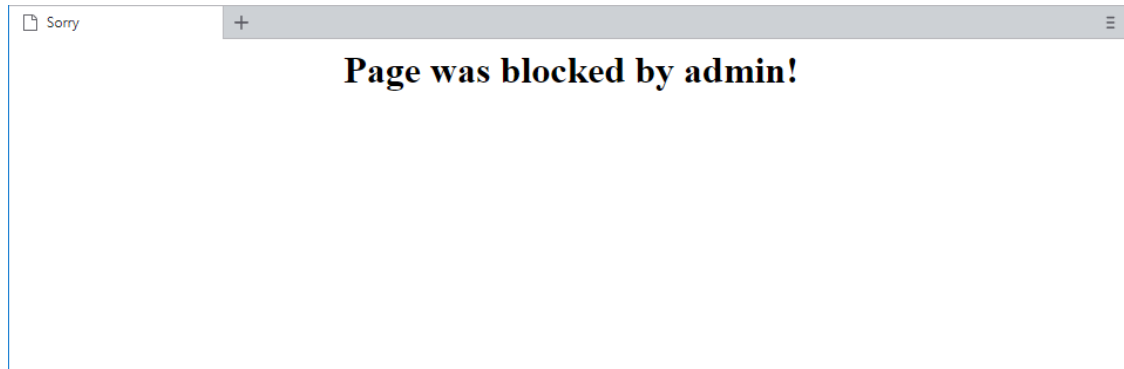


Figure 7: Default information page after redirection

You can prepare your custom Welcome/Banned page and upload it to the user module on *Welcome/Banned Page* in the *Configuration* section.

**Requirements** for the upload are the following:

- The uploaded file has to be an archive in *\*.tgz* or *\*.tar.gz* format (tarred and gzipped file). It can be done by native utilities in Linux or by e.g. 7-Zip application in Windows (freeware, take two steps: tar and then gzip).
- There has to be an *index.html* file in the root of the archive (no folder).
- The size of the archive has to be *1.5 kB* or less.

Choose the prepared file on the *Welcome/Banned Page* and click the *Update* button:

Figure 8: Upload custom welcome/banned page form

See the result of the successful upload in the next Figure. The uploaded page will be then shown to the user when the domain is blocked in the *Redirecting* mode.

Uploading Welcome/Banned Page to RAM... ok  
Extracting... ok

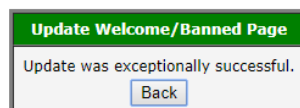


Figure 9: Successful upload of custom welcome/banned page

### 3. Related Documents

- |     |                                    |   |
|-----|------------------------------------|---|
| [1] | Advantech Czech:                   | <b>v2 Routers Configuration Manual</b> (MAN-0021-EN)<br>available from: <a href="https://ep.advantech-bb.cz">https://ep.advantech-bb.cz</a>   |
| [2] | Advantech Czech:                   | <b>SmartStart Configuration Manual</b> (MAN-0022-EN),<br>available from: <a href="https://ep.advantech-bb.cz">https://ep.advantech-bb.cz</a>  |
| [3] | Advantech Czech:                   | <b>SmartFlex Configuration Manual</b> (MAN-0023-EN),<br>available from: <a href="https://ep.advantech-bb.cz">https://ep.advantech-bb.cz</a>   |
| [4] | Advantech Czech:                   | <b>SmartMotion Configuration Manual</b> (MAN-0024-EN),<br>available from: <a href="https://ep.advantech-bb.cz">https://ep.advantech-bb.cz</a> |
| [5] | Advantech Czech:                   | <b>ICR-3200 Configuration Manual</b> (MAN-0042-EN),<br>available from: <a href="https://ep.advantech-bb.cz">https://ep.advantech-bb.cz</a>    |
| [6] | User Modules – Engineering Portal: | <a href="https://ep.advantech-bb.cz/user-modules">https://ep.advantech-bb.cz/user-modules</a>   |