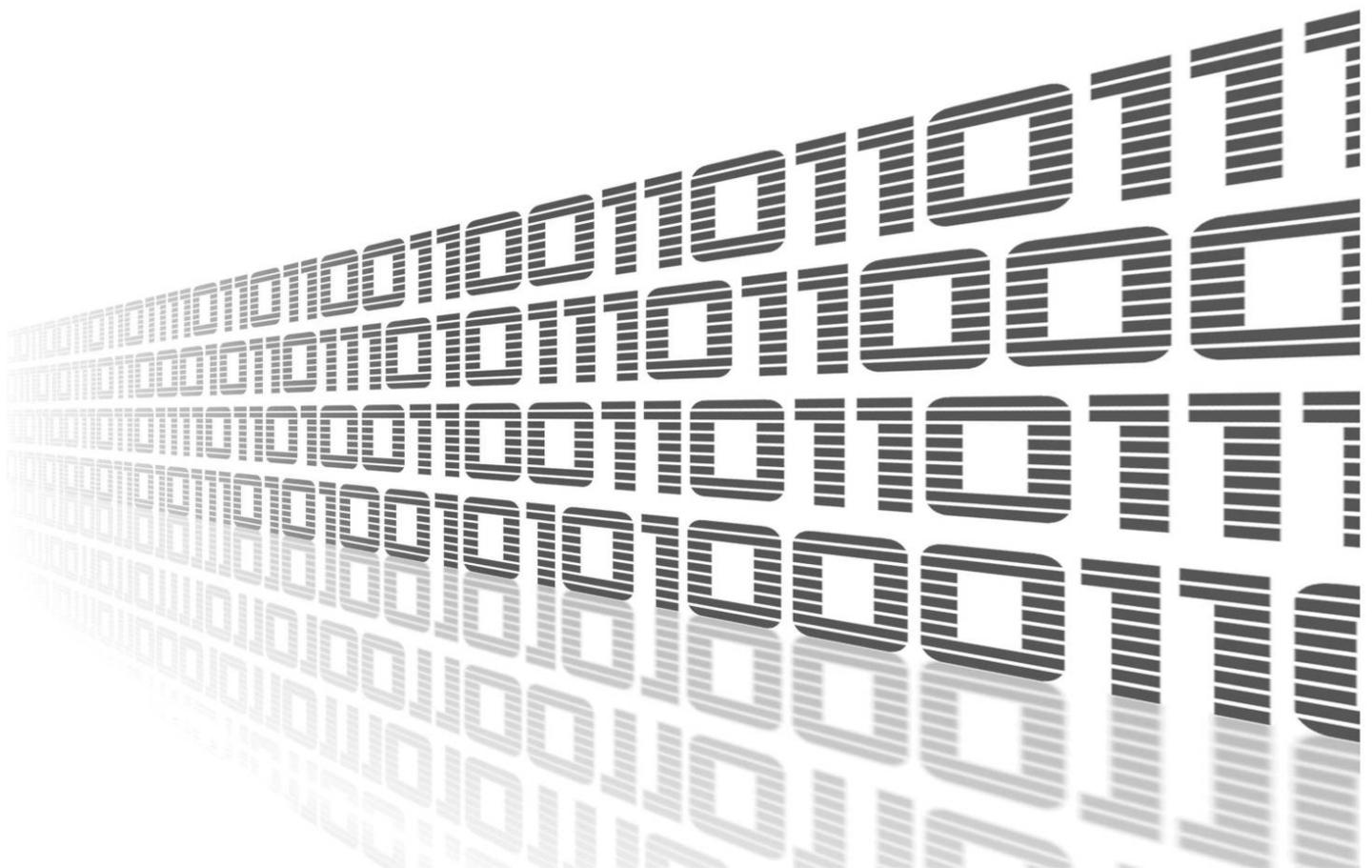




HTTP Authentication



© 2023 Advantech Czech s.r.o. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photography, recording, or any information storage and retrieval system without written consent. Information in this manual is subject to change without notice, and it does not represent a commitment on the part of Advantech.

Advantech Czech s.r.o. shall not be liable for incidental or consequential damages resulting from the furnishing, performance, or use of this manual.

All brand names used in this manual are the registered trademarks of their respective owners. The use of trademarks or other designations in this publication is for reference purposes only and does not constitute an endorsement by the trademark holder.

Used symbols

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

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

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

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

Contents

1. Changelog	1
1.1 HTTP Authentication Changelog	1
2. Description of user module	2
3. Configuration	3
3.1 Sample configuration	4
4. Related Documents	6

List of Figures

1 Scheme	2
2 Web interface	3
3 Sample configuration	5

List of Tables

1 Description of items	3
----------------------------------	---

1. Changelog

1.1 HTTP Authentication Changelog

v1.0.0 (2011-12-01)

- First release

v1.0.1 (2014-01-09)

- Added support of FW 4.0.0+

v1.0.2 (2015-03-19)

- Improved connection processing

v1.1.0 (2017-03-17)

- Recompiled with new SDK

v1.2.0 (2020-10-01)

- Updated CSS and HTML code to match firmware 6.2.0+

v1.2.1 (2022-02-04)

- Bugfixes (increased timeout and dynamic construction of HTTP response)

2. Description of user module



User module *HTTP Authentication* is not contained in the standard router firmware. Uploading of this user module is described in the Configuration manual (see [1, 2]).



The user module is v2 and v3 router platforms compatible.

Using this module, it is possible to add the process of authentication (identity verifying) to the server which does not provide this service. This means that in each subsequent attempt to access the server for which this module is activated (the server is specified in the configuration form of this module) is necessary to enter the IP address of the router and port number on which authentication takes place. Then it is always displayed the classic window asking user to enter login information. If entered data are identical with those which *HTTP Authentication* module requires, access to the server will go in a standard way. Otherwise user will see an error message *401 Unauthorised*.

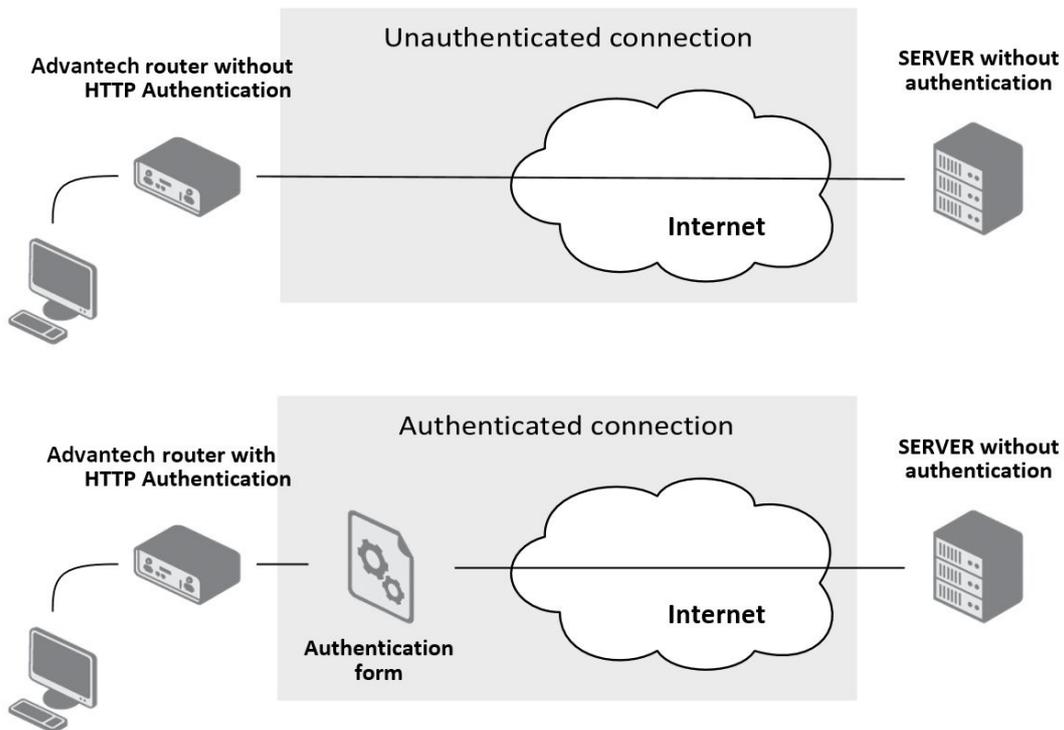


Figure 1: Scheme

For configuration *HTTP Authentication* user module is available web interface, which is invoked by pressing the module name on the *User modules* page of the router web interface. The left part of the web interface (ie. menu) contains only the *Return* item, which switches this web interface to the interface of the router.

3. Configuration

The actual configuration of the *HTTP authentication* user module configuration is performed via the form on the right of the web interface. The first item in the configuration form – *Enable HTTP authentication* – is used to activate this user module. Other items have the following meaning:

item	Description
Auth Server Listen Port	Port on which authentication takes place
Http Server IP Address	IP address of the server for which authentication is activated
Http Server Listen Port	Port where the server will be opened (usually 80)
Username	Username required for access to the above specified server
Password	Password required for access to the above specified server

Table 1: Description of items

The changes in settings will apply after pressing the *Apply* button.

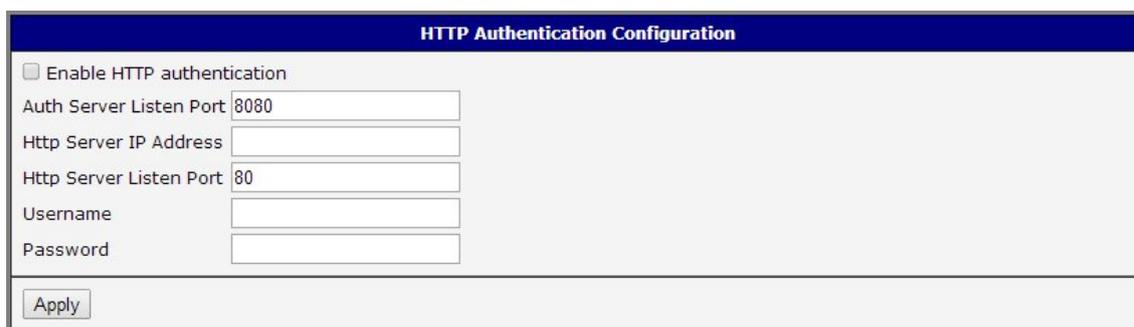
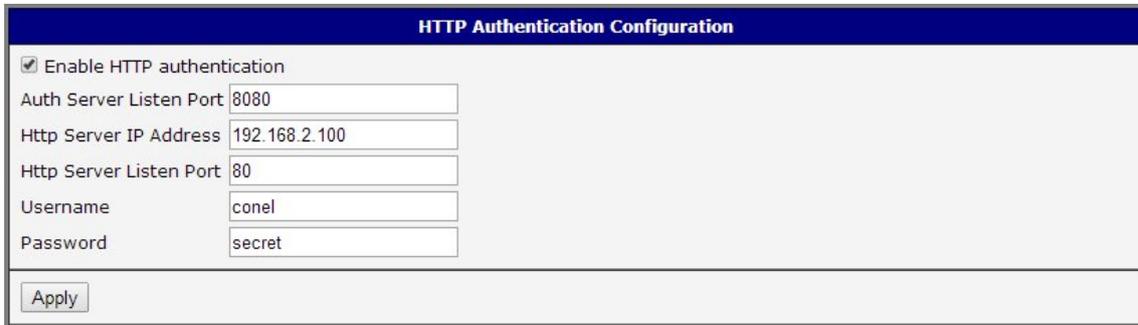


Figure 2: Web interface

3.1 Sample configuration

The figure below shows the situation in which authentication is required to access the server with IP address 192.168.2.100 and port number 80 (required username is "conel" and password is "secret"). The authentication process will run on port 8080. For authenticated access to the server user need to enter the IP address of the router with this user module and port number on which authentication takes place. Therefore, the complete address can have the following form: 10.0.3.188:8080.



The screenshot shows a configuration window titled "HTTP Authentication Configuration". It contains the following fields and values:

Field	Value
<input checked="" type="checkbox"/> Enable HTTP authentication	
Auth Server Listen Port	8080
Http Server IP Address	192.168.2.100
Http Server Listen Port	80
Username	conel
Password	secret

At the bottom left of the form is an "Apply" button.

Figure 3: Sample configuration

4. Related Documents

You can obtain product-related documents on *Engineering Portal* at icr.advantech.cz address.

To get your router's *Quick Start Guide*, *User Manual*, *Configuration Manual*, or *Firmware* go to the [Router Models](#) page, find the required model, and switch to the *Manuals* or *Firmware* tab, respectively.

The *Router Apps* installation packages and manuals are available on the [Router Apps](#) page.

For the *Development Documents*, go to the [DevZone](#) page.