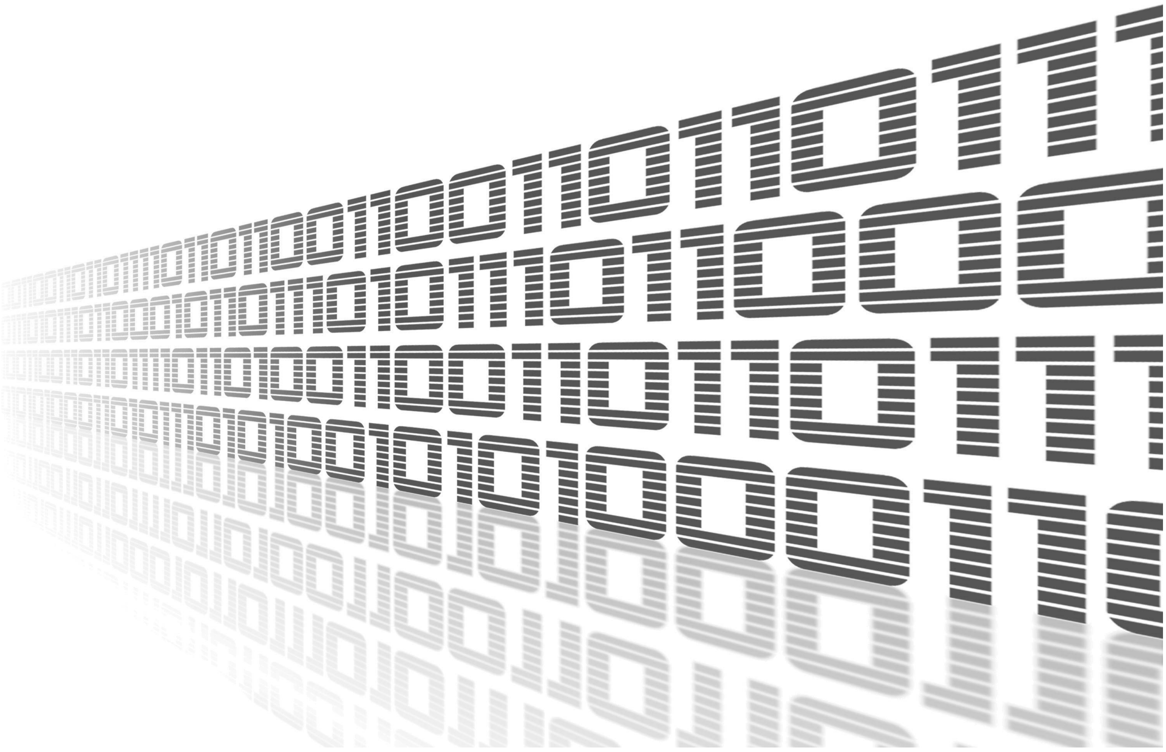
RouterApp

User Module

802.1X Authenticator

APPLICATION NOTE



ADVANTECH

www.lucom.de

19-01-21

Used symbols

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

Attention – Problems that can arise in specific situations.

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

Example – example of function, command or script.

TÜVRheinland®
COTI
ISO 9001

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic.
Document No. APP-0084-EN, revision from July 8, 2020. Released in the Czech Republic.

Contents

List of Figures

List of Tables

1. User Module 802.1X Authenticator

1.1 IEEE 802.1X Introduction

IEEE 802.1X is an **IEEE Standard** for **port-based Network Access Control** (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an **authentication mechanism** to devices wishing to attach to a LAN or WLAN. IEEE 802.1X defines the encapsulation of the **Extensible Authentication Protocol** (EAP) over IEEE 802, which is known as "EAP over LAN" or **EAPoL**.

802.1X authentication involves three parties: **a supplicant**, **an authenticator**, and **an authentication server**. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device which provides a data link between the client and the network and can allow or block network traffic between the two, such as an Ethernet switch or wireless access point; and the authentication server is typically a trusted server that can receive and respond to requests for network access, and can tell the authenticator if the connection is to be allowed, and various settings that should apply to that client's connection or setting. Authentication servers typically run software supporting the **RADIUS** and **EAP protocols**.

1.2 Module Description

This user module is not installed on *Advantech* routers by default. See the *Configuration Manual*, chapter *Customization –> User Modules*, for the description of how to upload a user module to the router.

802.1X Authenticator user module enables the router to act as an EAPoL Authenticator and authenticate other devices (supplicants) connecting over a (wired) LAN interfaces. For the functional diagram of this authentication see Figure 1.

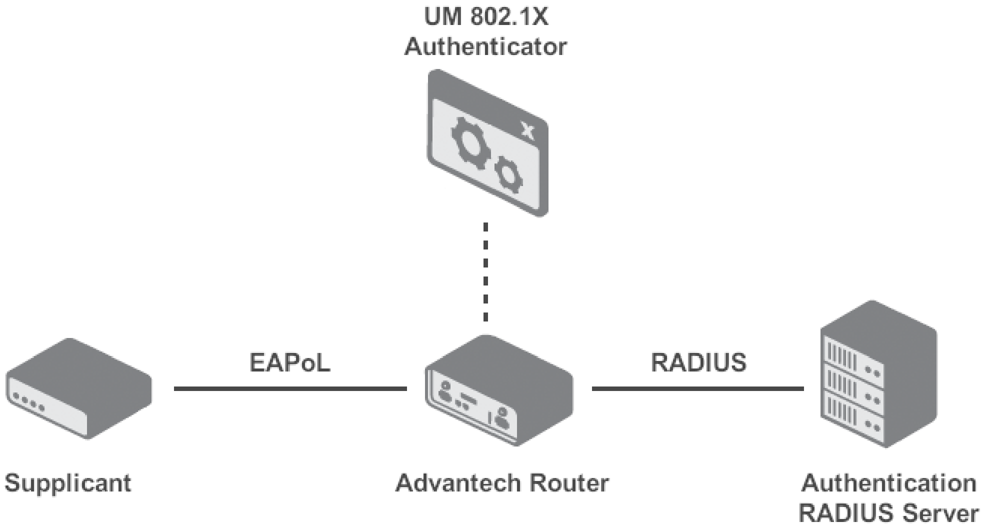


Figure 1: Functional Diagram

The connecting device (a supplicant) can be another router, managed switch or other device supporting the IEEE 802.1X authentication.

Note that this user module applies to wired interfaces only. For wireless (WiFi) interfaces is this functionality included in the WiFi Station (STA) configuration, when Authentication it set to 802.1X.

1.3 Installation

The latest version of *802.1X Authenticator* user module can be downloaded from the Engineering Portal [EP] at `https://ep.advantech-bb.cz/products/software/user-modules#802.1XAuthenticator`.

In the GUI of the router navigate to *Customization -> User Modules* page. Here choose the downloaded module's installation file and click to the *Add or Update* button.

Once the installation of the module is complete, the module's GUI can be invoked by clicking the module name on the *User modules* page. In Figure 2 is shown the main menu of the module. It has the *Status* menu section, followed by the *Configuration* and *Customization* menu sections. To return back to the router's web GUI, click on the *Return* item.

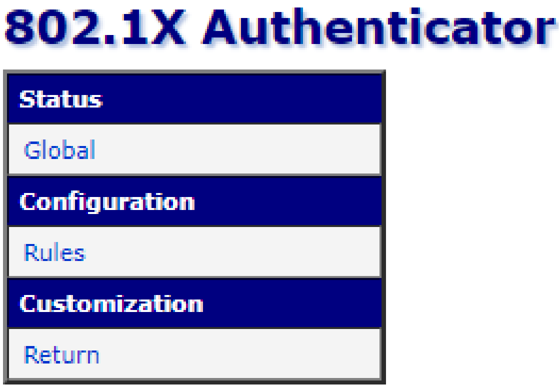
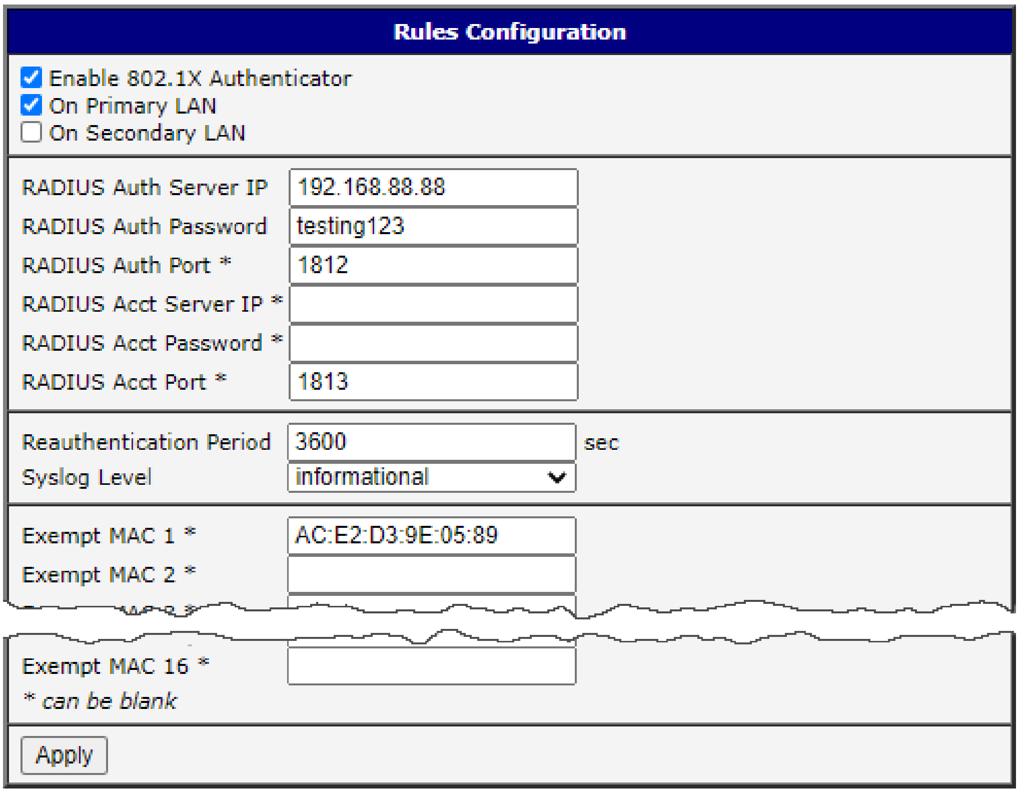


Figure 2: Main menu

1.4 Module Configuration

To configure the *802.1X Authenticator* user module installed on an Advantech router, go to the *Rules* page under the *Configuration* menu section of module's GUI. On this page, tick the *Enable 802.1X Authenticator* together with the required LAN interface. Configure the RAIDUS credentials and other settings, see Figure 3 and Table 1.



Rules Configuration

☑ Enable 802.1X Authenticator
☑ On Primary LAN
□ On Secondary LAN

RADIUS Auth Server IP	192.168.88.88
RADIUS Auth Password	testing123
RADIUS Auth Port *	1812
RADIUS Acct Server IP *	
RADIUS Acct Password *	
RADIUS Acct Port *	1813
Reauthentication Period	3600 sec
Syslog Level	informational
Exempt MAC 1 *	AC:E2:D3:9E:05:89
Exempt MAC 2 *	
Exempt MAC 16 *	

** can be blank*

Figure 3: Configuration Examle

Item	Description
Enable 802.1X Authenticator	Enables the 802.1X Authenticator functionality Once enabled, you also need to specify on which interface this should be activated (see bellow).
On ... LAN	Activates the authentication for a given interface. When disabled, any MAC address can connect to that interface. When enabled, authentication is required prior communication on that interface.

Continued on the next page

Continued from previous page

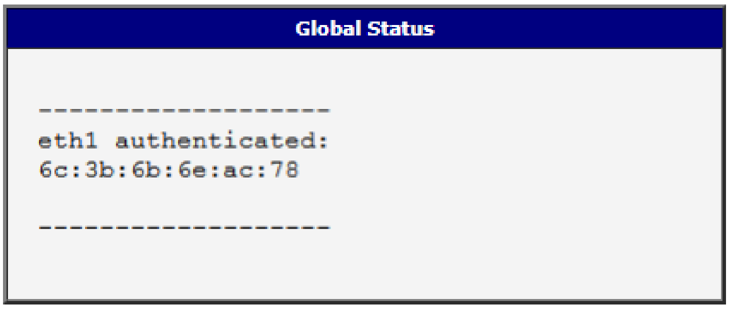
Item	Description
RADIUS Auth Server IP	IP address of the authentication server.
RADIUS Auth Password	Access password for the authentication server.
RADIUS Auth Port	Port for the authentication server.
RADIUS Acct Server IP	IP address of the (optional) accounting server.
RADIUS Acct Password	Access password for the (optional) accounting server.
RADIUS Acct Port	Port for the (optional) accounting server.
Reauthentication Period	Limit the authentication for a given number of seconds. To disable reauthentication, use "0".
Syslog Level	Set verbosity of information sent to syslog.
Exempt MAC x	Set up MAC addresses which shall not be subject to authentication. These will not be required to authenticate even when authentication is activated.

Table 1: Description of Configuration Items

If you want to configure another Advantech router to act as the supplicant, configure the appropriate LAN interface on the LAN configuration page. On this page enable the *IEEE 802.1X Authentication* and enter an *Identity* and *Password* of a user that is provisioned on the RADIUS server.

1.5 Module Status

Status messages of the module can be listed on the Global page under the Status menu section, see Figure 4. It contains information which clients (MAC addresses) are authenticated for each interface.



```
--------------------
eth1 authenticated:
6c:3b:6b:6e:ac:78

--------------------
```

Figure 4: Status Messages

1.6 Known Issues

Known issues of the module are:

- This module requires the firmware version 6.2.5 or higher.
- The router firewall cannot block DHCP traffic. Hence, when an unauthorized device connects, it will anyway get a DHCP address. All further communication will be blocked, but the DHCP server will assign it an address regardless the authentication status.

2. Related Documents

[1] Advantech Czech: **v2 Routers – Configuration Manual** (MAN-0021-EN)
[2] Advantech Czech: **SmartFlex – Configuration Manual** (MAN-0023-EN)
[3] Advantech Czech: **SmartMotion – Configuration Manual** (MAN-0024-EN)
[4] Advantech Czech: **SmartStart – Configuration Manual** (MAN-0022-EN)
[5] Advantech Czech: **ICR-3200 – Configuration Manual** (MAN-0042-EN)

[EP] Product related documents and applications can be obtained on *Engineering Portal* at `https://ep.advantech-bb.cz/` address.