DEFAULT LOGIN: URL: https://192.168.1.88 User: admin Password: 1234

Overview

This Quick Start Guide shows how to set up and configure this device to provide a strong authentication server to your RADIUS devices.
With the **virtual appliance edition**, you can directly configure the IP settings using the embedded console and skip to point 4.
More documentation is available using the "**? Help**" link in the top right corner once you are logged in.

1. Connect the hardware

1. Using the Ethernet cable provided, connect the ETHERNET port to a computer or your network for initial configuration.
2. Using the USB cable provided, connect the mini USB to a powered USB port. Alternatively, you may also power the device using an optional 5V/1A power supply.

1.1. LEDs

- The power LED turns steady blue when the power is connected.
- The Ethernet LED turns on if the Ethernet port is properly connected, and blinks when there is traffic.

2. Access the Web configurator

Use a recent version of Firefox, Google Chrome or Internet Explorer with JavaScript enabled and pop-up blocking disabled.

2.1. Set up your computer's IP address

Write down your computer's current IP settings before you change them.
First, set your computer to use a static IP address in the 192.168.1.100-192.168.1.200 range with a subnet mask of 255.255.255.0. This ensures that your computer can communicate with the device.

2.2. Log into the Web interface

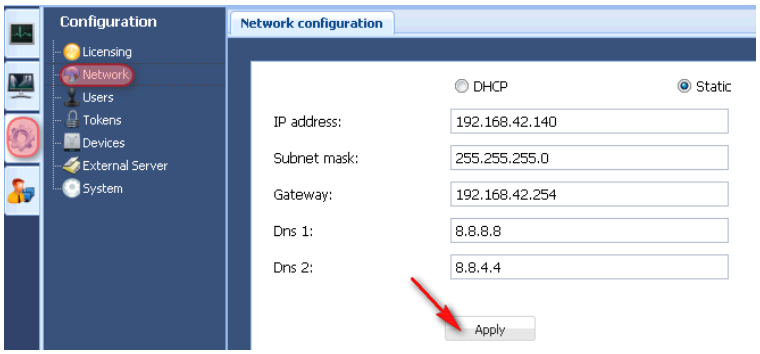
1. Launch your web browser. Enter **192.168.1.88** (the **multiOTP®** default IP address) as the address. You have to accept the self-signed SSL certificate to go further.
2. Type the default username **admin** and the default password **1234**, and click **Login**.
3. The dashboard screen appears, saying you have logged in with the default password.
4. It's strongly recommended to change the default password. Click on "changing the password" on the first page displayed, enter your new password twice and accept the change by clicking **Apply**. Be sure to record the new password and keep it in a safe place.

   If you change the password and then forget it, you will need to reset the device using the RESET button.
   Power off the device, hold the RESET button during power on, and keep the RESET button held until the LEDs 1 and 4 are fixed and LEDs 2 and 3 are blinking very quickly (10 times per seconds).
   Now release the RESET button, the device will reboot to the factory state.
5. Type again the default username **admin** and your new password, and click **Login**.
6. The dashboard screen appears.

3. Configure IP settings

You need to set the device IP address to be in the same subnet as your usual network.

1. Click on the configuration wheel on the left. The configuration submenu appears. Click **Network** in the submenu. The Network settings appears.



   Select **DHCP** if you want to have a DHCP server on your network assign an IP address to the device. Before you apply the change, the device will try to show you the IP address which will be attributed by the DHCP server.

   If you want to use a specific IP address, select **Static** and enter it along with the subnet mask, the gateway IP address and the DNS IP address(es). Click **Apply** and the device restart using now the new IP settings.

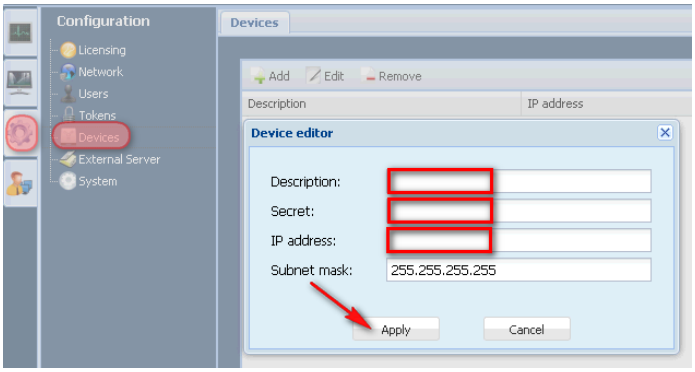
2. If you changed your computer's IP address before, return it to its previous setting.

The device is now ready to connect to your switch or router. You can do this now.

If the **multiOTP®** device cannot communicate with the network, ensure that the device is using an IP address on the same subnet as the rest of the network.

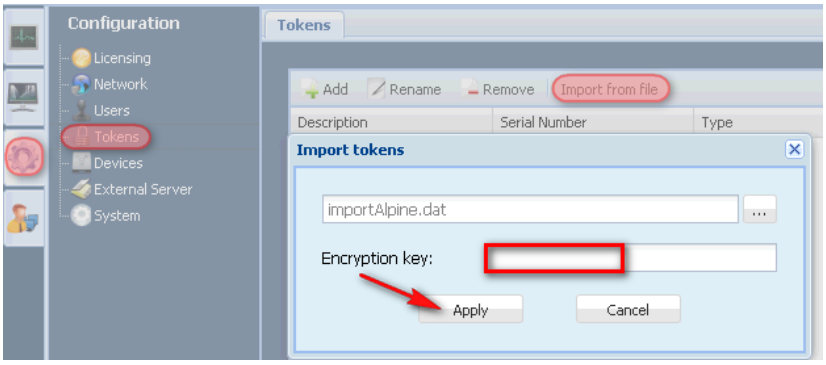
4. Configure devices

You will have to add the device(s) that will make RADIUS requests to the **multiOTP®** device on the standard **1812 RADIUS port**.
Click on the configuration wheel on the left. The configuration submenu appears. Click **Devices** in the submenu. The Devices tab appears.
Click on **Add** to add a new device (like a firewall if you want to have VPN with strong authentication). Click **Apply** when all fields are filed.



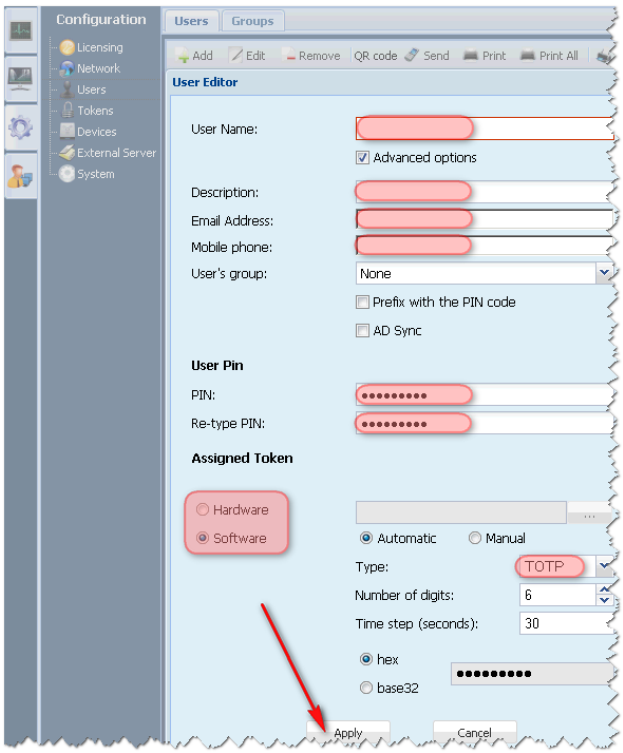
5. Import hardware tokens (if any)

With **multiOTP®**, you can use any OATH certified tokens, and a lot of compatible tokens (like Authenex, ZyWALL OTPv2, etc.).
Click on the configuration wheel on the left. The configuration submenu appears. Click **Tokens** in the submenu. The Tokens tab appears.
Click on **Add** to manually add new hardware tokens, or simply click on **Import from file** if you have a provisioning file. Type the **encryption key** if the file is encrypted, and click on **Apply** to import the tokens.



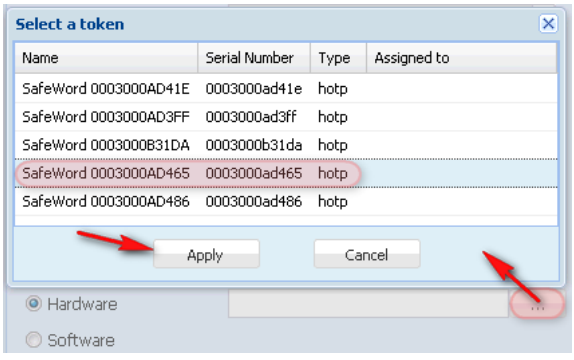
6. Create users

To create users, click on the configuration wheel on the left. The configuration submenu appears. Click **Users** in the submenu. The Users tab appears. Click on **Add** to add a new user. The **User Editor** appears without the advanced options enabled. Simply type the user name you want to create, or enable the **Advanced options** if you want to setup more options. **By default, a PIN code is enabled for each user**.



Without **Advanced options**, the user is created with a random prefix PIN, and the software token is TOTP based with 6 digits.

If you want to assign a hardware token, select **Hardware**, click on the **[…]** button and select the token you want to assign to the user.



If you have created user(s) with TOTP or HOTP software token, you can now print the provisioning QRcode(s).