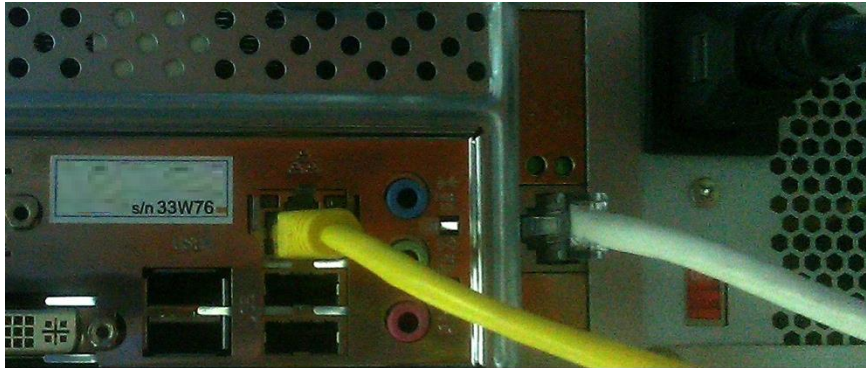


## UserGate Web Filter Appliance Quick start

UserGate Web Filter Appliance units are pre-configured, so you need to perform only a few steps to get started:

1. Connect the LAN interface of the UserGate Filter Appliance to the computer network and connect the WAN interface to the Internet.



2. Make sure that your computer has an IP address which belongs to the following network 192.168.1.0/24. If this is not the case, give your computer an address in the range of 192.168.1.1 to 192.168.1.253, for example: 192.168.1.252 with mask 255.255.255.0.
3. Connect to the web console for UserGate Web Filter Appliance at the following address: **http://192.168.1.254:4040/admin/**. Default settings:

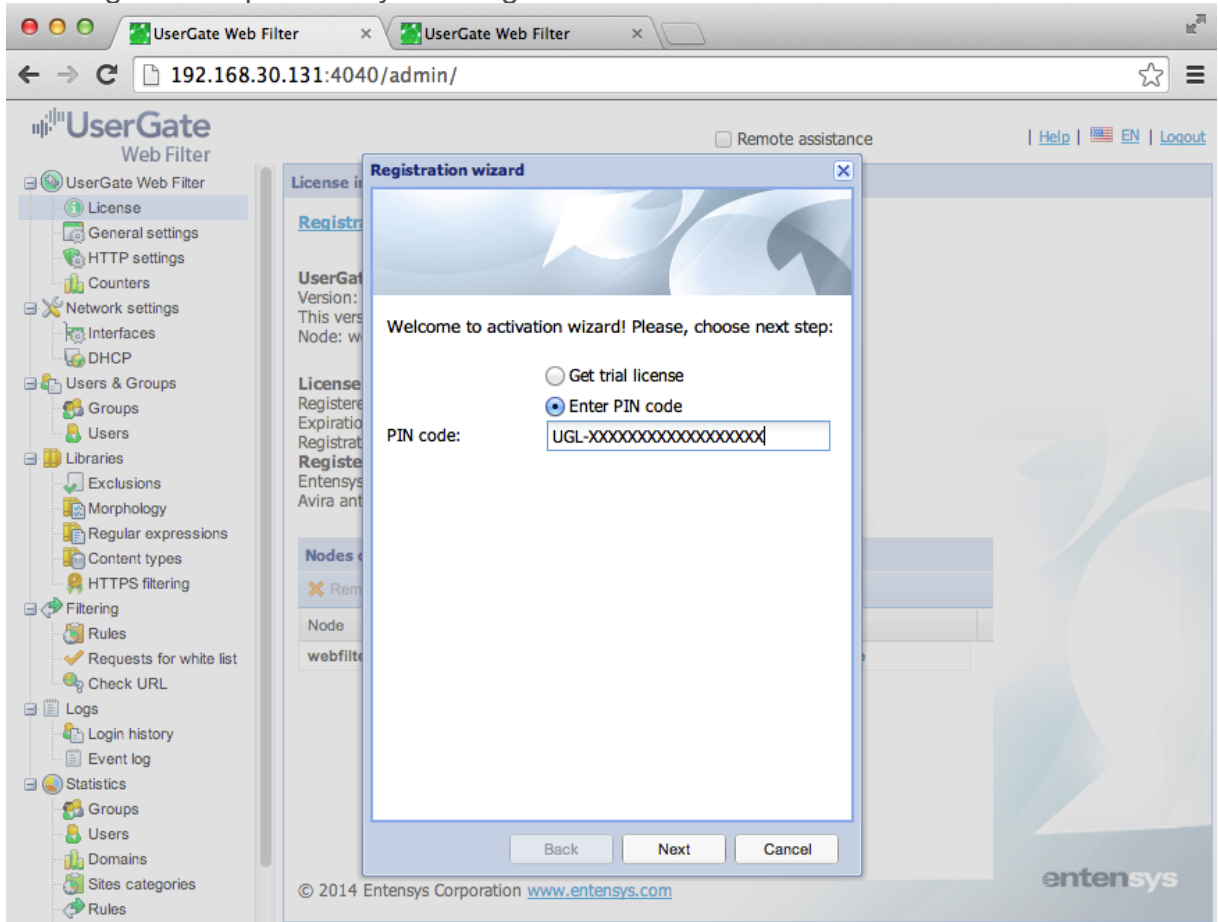
**server address** - <http://192.168.1.254:4040/admin/>;

**username** – "Admin" (with a capital A);

**password** – "admin" (with a lowercase a).

You can change the password later.

## 4. Register the product by entering the PIN code.



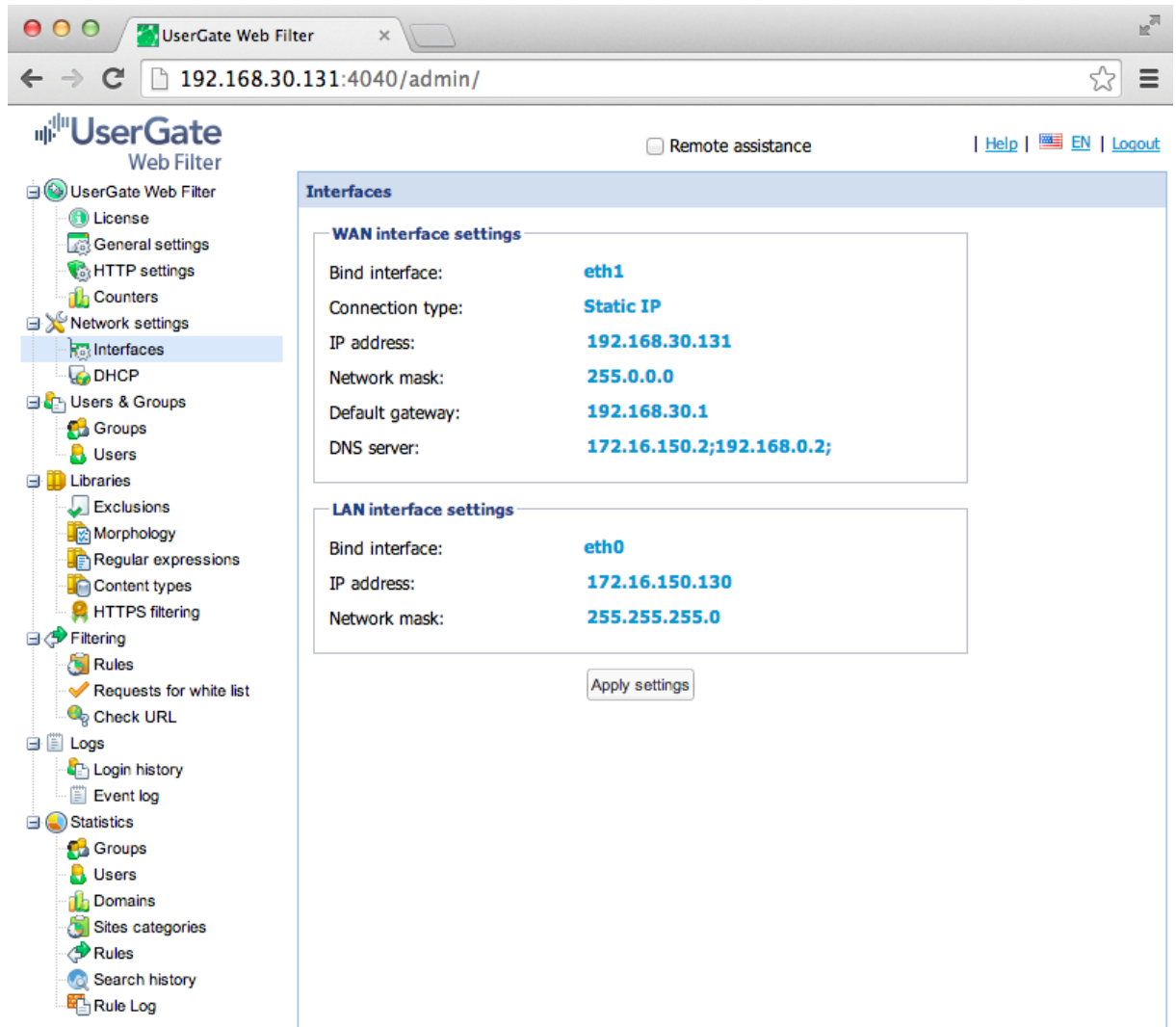
## 5. Activate users on the Users tab.

The screenshot shows the UserGate Web Filter administration interface. The browser address bar displays `192.168.30.131:4040/admin/`. The left sidebar contains a navigation tree with the following items: UserGate Web Filter, License, General settings, HTTP settings, Counters, Network settings, Interfaces, DHCP, Users & Groups, Groups, Users (highlighted), Libraries, Exclusions, Morphology, Regular expressions, Content types, HTTPS filtering, Filtering, Rules, Requests for white list, Check URL, Logs, Login history, Event log, Statistics, Groups, Users, Domains, Sites categories, and Rules. The main content area is titled "Users" and features a table with the following data:

	User name	Group	Lists	Rules	IP list
<input checked="" type="checkbox"/>	everybody	default	HTTPS intercept...	Default rule	1.1.1-255.255...

At the bottom of the interface, there is a pagination control showing "Page 1 of 1" and a "Filter" input field.

6. Specify IP addresses for LAN and WAN what are correct for your network.



**Important:** If you change the IP address of the local network, you will need to reconnect to the web console at the new address: `http://new-IP-address/admin/`.

**Important:** If you have Appliance or Virtual Appliance with only one network interface and you want to change IP address to a different subnet, you must have the IP addresses of both subnets assigned to your computer.

7. Edit the redirect URL for blocked HTTP requests on the HTTP settings page. Specify a new LAN address instead of 127.0.0.1: <http://NEW-LAN-IP:8001/>

The screenshot shows the UserGate Web Filter administration interface. The browser address bar displays `192.168.70.90:4040/admin/`. The left sidebar contains a navigation tree with 'HTTP settings' selected. The main content area is titled 'HTTP settings' and is divided into three sections:

- HTTP filtering:** AD block. Automatic update: **Enabled**. Entensys lists: Entensys lists version: 108 Last update: 2014/08/24. **Blocked requests redirect address: <http://192.168.70.90:8001/>** (highlighted in red).
- Cache settings:** Cache mode: **RFC**. Max cacheable object size (Mb): **1**. RAM size (Mb): **512** (0.5%). Disk cache size (Mb): **2048** (15.2%).
- ICAP Settings:** Use next ICAP server: **Disabled**. Next ICAP server (REQMODE): [Click to enter value](#). Next ICAP server (RESPMODE): [Click to enter value](#).

At the bottom of the browser window, the address bar shows `192.168.70.90:4040/admin/#`.

8. Set the IPv4-address for blocked DNS requests on the General settings page to appliance's LAN IP address.

The screenshot shows the UserGate Web Filter administration interface. The browser address bar displays `172.16.150.130:4040/admin/`. The main content area is titled "General settings" and contains several configuration sections:

- DNS settings:**
  - Blocked requests IP address: **172.16.150.130** (highlighted with a red box)
  - redirect to (IPv4):
  - Blocked requests IP address redirect to (IPv6): `::1`
  - Allow recursive DNS requests: **Disabled**
  - Use DNS cache: **Disabled**
  - Answer for unknown users: **No answer**
  - Set maximum TTL for DNS records: **86400**
  - DNS response if cloud URL filtering is not available: **Block**
  - Use DNS servers from list: **Enabled**
- General settings:**
  - Timezone: **Asia/Novosibirsk**
  - If no license, all requests are: **Blocked**
  - Log level: **Error**
  - Download logs
  - Import settings:
  - Export settings
- Statistics server:**
  - Collect statistic: **Enabled**
  - Status: **Statistics server is connected**
  - Records in cache: 0
- Radius server settings:**
  - Status: **Disabled**
  - IP-address: **127.0.0.1**
  - Radius passphrase: **secret**

At the bottom of the DNS settings section, there is a table for "DNS servers IP addresses":

DNS servers IP addresses
172.16.150.2
8.8.8.8

9. Change password for user Admin. Do not use simple passwords.
10. Change users' computer settings to enable filtering with one of the following methods:
  - Change Default Gateway on users' computers, so all traffic flows through UserGate Web Filter appliance.
  - Configure proxy settings in users' browsers. For HTTP and HTTPS proxy – appliance IP address, port 8090.

Your UserGate Web Filter Appliance is now ready. For more detailed configuration, consult the user guide.

In case of technical problems please refer to the technical support area at <http://entensys.com/support>.