Authorization by IP address

Configuring Authorization by IP

Authorization by IP implies that an authorized user will gain access to Internet resources without entering a username and password, but simply by initiating a connection to these resources.

You can also authorize network devices (such as CCTV cameras, network printers, etc.) that are located in broadcast domains other than SafeUTM, and that require Internet access.

If the device is a router and SNAT is enabled on it, then when its external IP is authorized in UTM, all users behind this router will gain Internet access.

Users who are behind the router in the local UTM network cannot be authorized using the IP address - MAC address bind, since the router does not handle L2-level traffic.

If authorization by IP address is configured, this IP will not be issued by **DHCP**.

To authorize a user by IP address:

- 1. **Create** a user that will be authorized by IP in SafeUTM or **import** a user from Active Directory.
- 2. Go to Users -> Authorization -> IP and MAC authorization.
- 3. Create a binding rule **IP address <--> User**, as shown in the screenshot.

Authorization

| General | IP and MAC authorization | Subnet a | |
|-----------------|--------------------------|----------|--|
| Adding an | authorization rule | | |
| Jane Smith | | * | |
| Specify IP only | y, MAC only, or both. | | |
| 192.168.150 | 0.50 | | |
| Get MAC by | y IP | | |
| MAC | | | |
| Permane | ntly authorized | | |
| Comment | | | |
| Save | Cancel | | |

The user's IP address is to be used when creating a session. The computer/device's IP address must match the one specified in the rule.

If the user is network equipment (video cameras, servers, etc.), it is recommended to select **Permanently Authorized**, in which case the user session will be created after the UTM is turned on, and the network equipment does not need to make a web request. For such equipment, it is recommended to configure a static IP address or DHCP with an IP address binding.

This is required, for example, for resources **published via DNAT**.

After the user makes a web request, a session with the IP authorization type will automatically be created on UTM in **Monitoring -> Authorized Users**.



For sessions with an IP authorization type, the **MAC address** field is not filled in, because, with this type of authorization, there is already an IP address required to create an authorization session.

You can use device search to automatically create users when they try to access the Internet. To do this, see the **Netscan** article.

Only one device can be authorized under one user by IP address (simultaneously with this type of authorization, two more devices can be authorized under one user by any other authorization method).

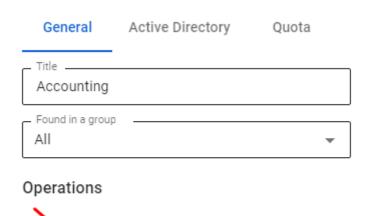
Adding Group of Devices with Authorization by IP

You can add users from a range of IP addresses (for example, a network distributed by access points to wireless devices over Wi-Fi). To do this, you need to follow these steps:

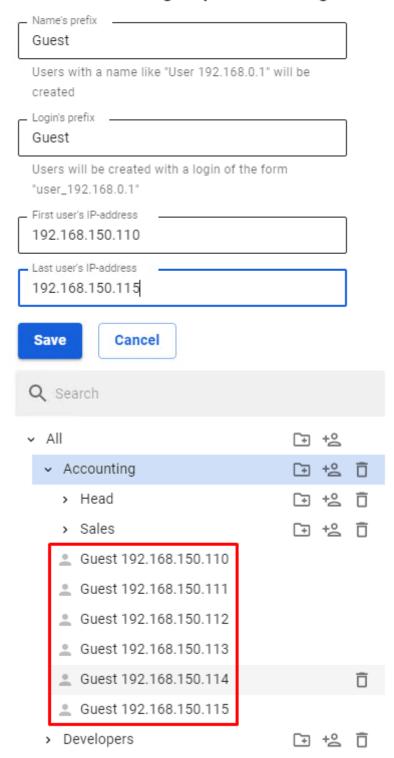
- 1. Create a new group in the user tree.
- 2. Select a group from the user tree to which you want to add devices.
- 3. In the **General** tab, click **Create Users**.

A window opens with the settings of the users created. Fill in the following fields:

- 1. Name Prefix. Users will be created with names of the type "User IP address ".
- 2. **Login prefix.** Users will be created with logins of the type "user_ip-address".
- 3. IP addresses of the first and last users.



Create users to group "Accounting"



If some IP addresses from the range are already used by other SafeUTM users, they will be skipped during creation, and as a result, fewer users will be created than addresses in the range.

Users will be created with the settings of the created group and an IP address from the range. In addition to the user tree, in the section **Users -> Authorization -> IP and MAC authorization** for each user, a binding rule **IP address <--> User** will be created automatically, as shown in the

screenshot:

Head MAC authorization

Subnet authorization

Rows per page: 10 ▼ 1-8 of 8 < > Q III

IP address MAC address ↑ User Always logged Comment Operations

192.168.150.110 - Created automatically by range

| IP address | MAC address ↑ | User | Always logged | Comment | Operations |
|-----------------|---------------|------------------------------|---------------|--------------------------------|-------------------------|
| 192.168.150.110 | - | Quest 192.168.150.110 | | Created automatically by range | (b) / i |
| 192.168.150.111 | _ | Quest 192.168.150.111 | | Created automatically by range | (b) / i |
| 192.168.150.112 | - | Quest 192.168.150.112 | () | Created automatically by range | (b) / (i) |
| 192.168.150.113 | - | Quest 192.168.150.113 | - | Created automatically by range | (b) / (i) |
| 192.168.150.114 | - | Quest 192.168.150.114 | () | Created automatically by range | (b) / (i) |
| 192.168.150.115 | _ | Quest 192.168.150.115 | () | Created automatically by range | (b) / (i) |
| | | | | | |

If you use IP authorization with static binding in DHCP, it is preferable to transfer such rules to **authorization by MAC address**.

Revision #6 Created 22 August 2022 14:57:46 by Val Redman Updated 12 October 2022 00:01:06 by Val Redman