Authorization by MAC address

This type of authorization is suitable for those devices whose location changes from time to time between local networks within the organization (for example, employees' work laptops) or network devices that are issued an IP address via DHCP, on which IP+MAC binding is not configured.

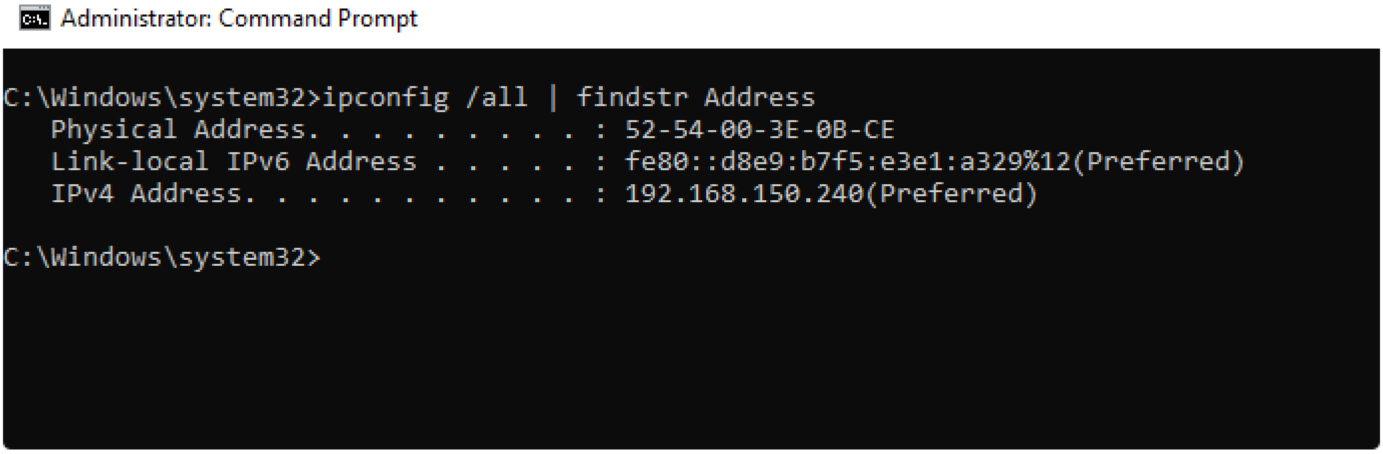
In order for a device to be authorized on UTM by MAC address, they must both be in the same broadcast domain, and UTM serves as the gateway for the devices.

Users who are behind the router in the local UTM network cannot authorize by MAC address, since the router breaks broadcast domains and does not process L2-level traffic. Such users can authorize only by IP address.

Configuring MAC Authorization

To authorize a user by MAC address, you need to do the following:

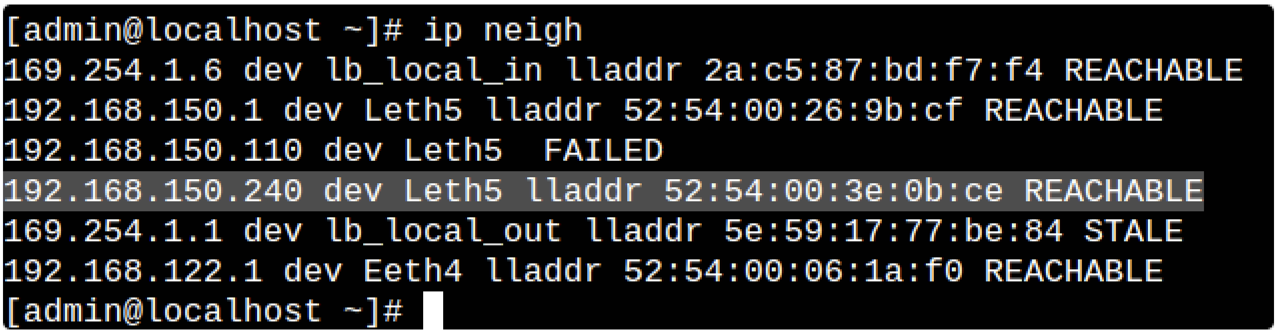
1. You need to find out the MAC address of the device. To do this, in the Windows command prompt, type the command: `ipconfig /all |  findstr  Address`



```
C:\Windows\system32>ipconfig /all | findstr Address
   Physical Address. . . . . . . . . : 52-54-00-3E-0B-CE
   Link-local IPv6 Address . . . . . : fe80::d8e9:b7f5:e3e1:a329%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.150.240(Preferred)

C:\Windows\system32>
```

2. Make sure that the computer and UTM are in the same broadcast domain.
To do this, on UTM in Server Management -> Terminal section, enter the command: `ip neigh`



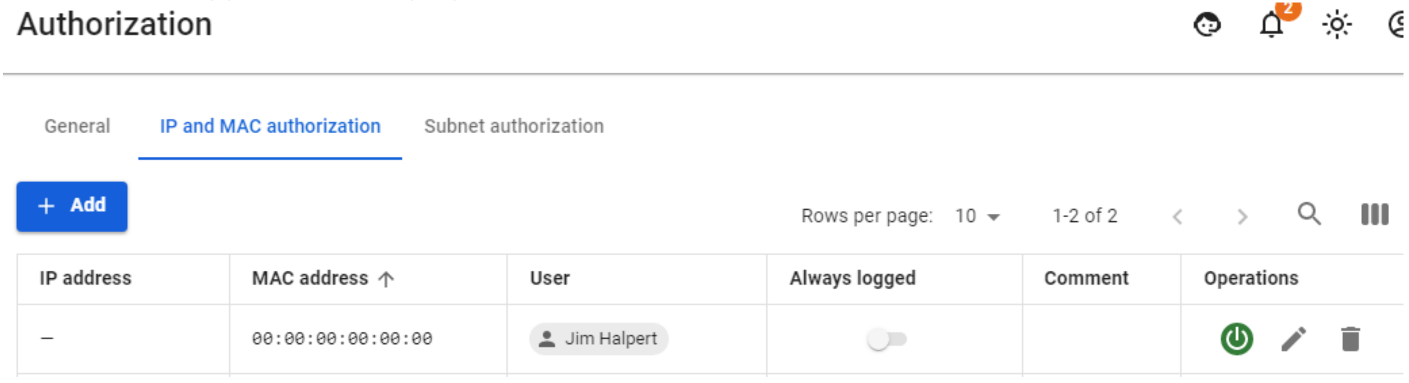
```
[admin@localhost ~]# ip neigh
169.254.1.6 dev lb_local_in lladdr 2a:c5:87:bd:f7:f4 REACHABLE
192.168.150.1 dev Leth5 lladdr 52:54:00:26:9b:cf REACHABLE
192.168.150.110 dev Leth5  FAILED
192.168.150.240 dev Leth5 lladdr 52:54:00:3e:0b:ce REACHABLE
169.254.1.1 dev lb_local_out lladdr 5e:59:17:77:be:84 STALE
192.168.122.1 dev Eeth4 lladdr 52:54:00:06:1a:f0 REACHABLE
[admin@localhost ~]#
```

> This command outputs the UTM's ARP table, and the presence of an entry with the device MAC address and REACHABLE status indicates L2 availability between UTM and the device.

3. Create a binding rule **User <--> MAC address** in **Users -> Authorization -> IP and MAC authorization:**

> It is not possible to set up permanent authorization for MAC authorization.
> This is technically impossible because an IP address is required to create an authorized session. Therefore, it is recommended to use MAC authorization in combination with a **DHCP server**.

The result can be viewed in **Monitoring -> Authorized users**, where a session with the MAC authorization type will be displayed.



IP address	MAC address ↑	User	Always logged	Comment	Operations
–	00:00:00:00:00:00	Jim Halpert			

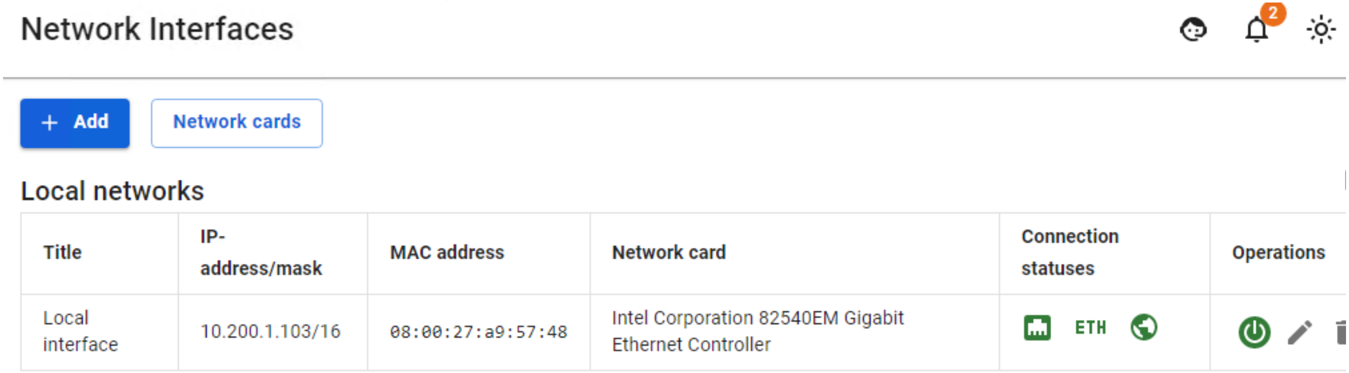
MAC authorization behavior when moving a device between local networks

In organizations, there is often a situation when it is necessary to move between local networks with a laptop and at the same time always stay online. In such cases, authorization by MAC address works perfectly well.

> You must have your own DHCP server configured or on SafeUTM. In the distributed credentials, the gateway should be the local SafeUTM interface.

Let's take as an example a situation where a user `Dwight Schrute` needed to move with a laptop between local networks:

- There are local interfaces configured on UTM as follows:

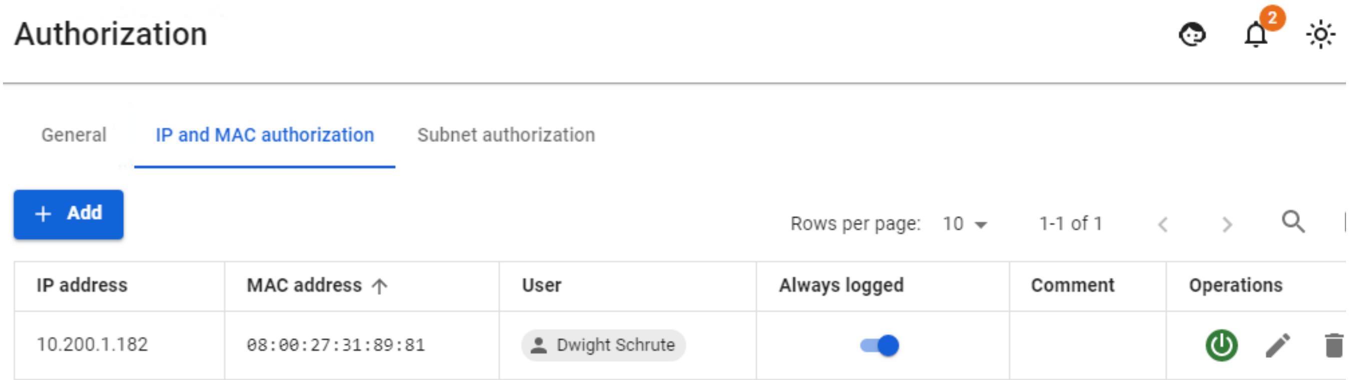


Network Interfaces

Local networks

Title	IP-address/mask	MAC address	Network card	Connection statuses	Operations
Local interface	10.200.1.103/16	08:00:27:a9:57:48	Intel Corporation 82540EM Gigabit Ethernet Controller	ETH	

- This user has a MAC address authorization rule configured:

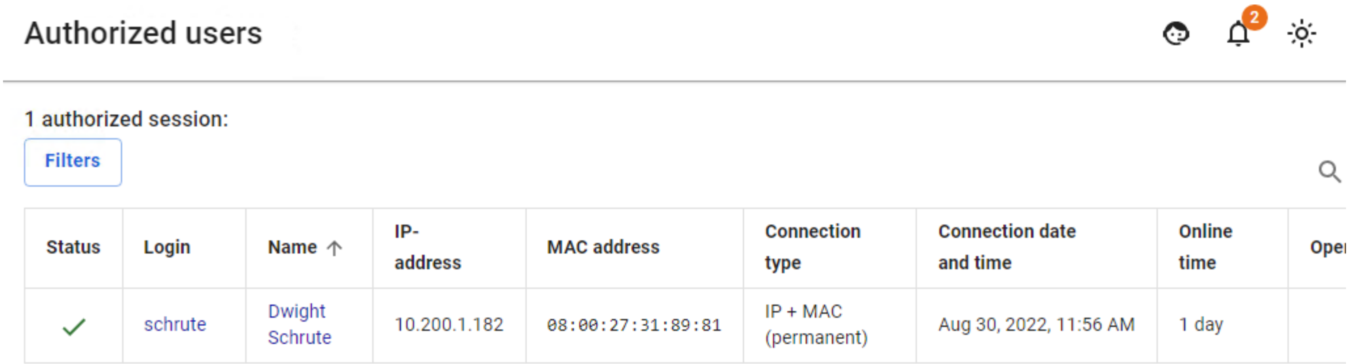


Authorization

Rows per page: 10 1-1 of 1

IP address	MAC address ↑	User	Always logged	Comment	Operations
10.200.1.182	08:00:27:31:89:81	Dwight Schrute	●		

- He also has one active session in the **Authorized Users** section:



Authorized users

1 authorized session:

Status	Login	Name ↑	IP-address	MAC address	Connection type	Connection date and time	Online time	Oper
✓	schrute	Dwight Schrute	10.200.1.182	08:00:27:31:89:81	IP + MAC (permanent)	Aug 30, 2022, 11:56 AM	1 day	

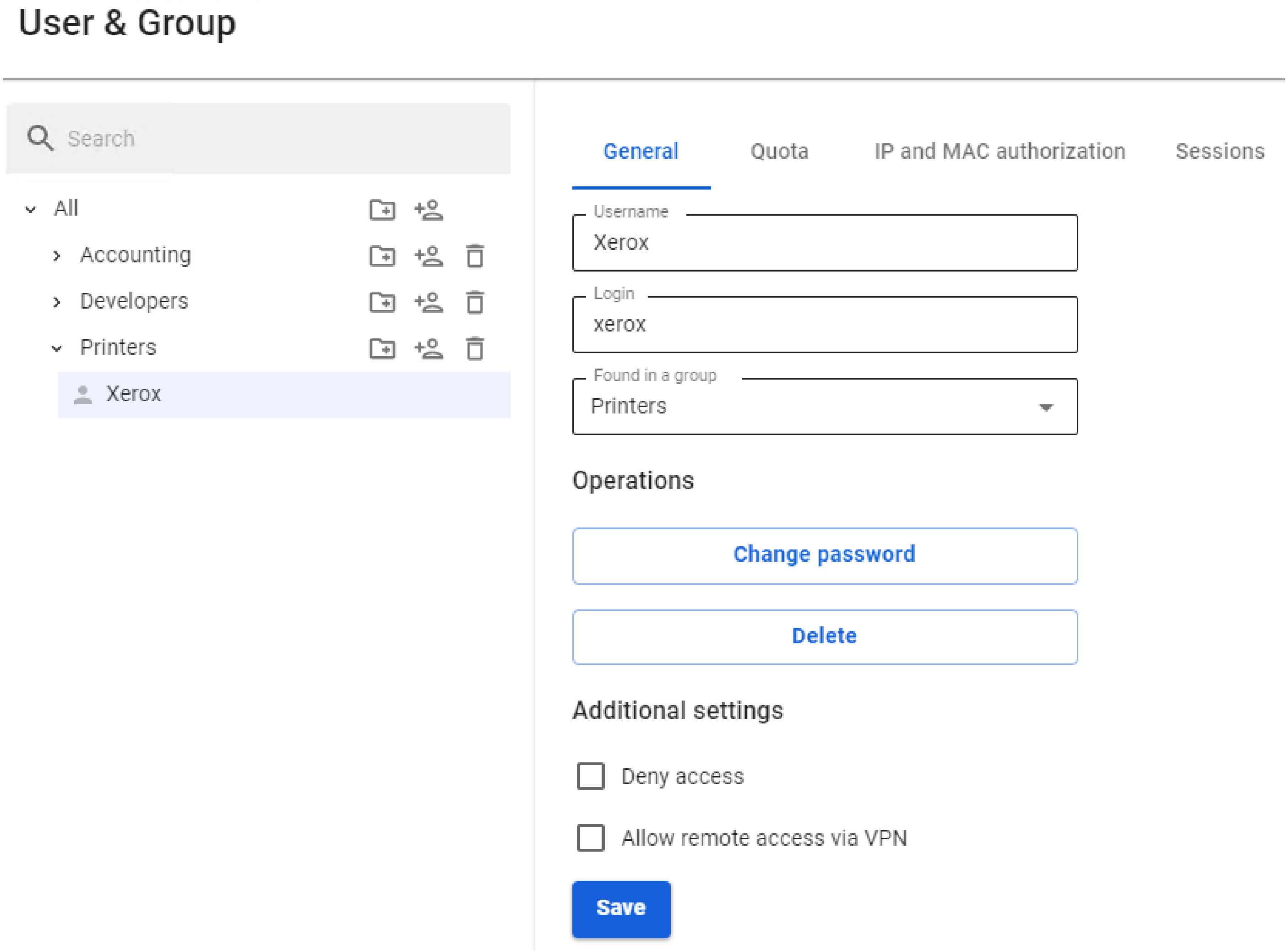
- Then the user moves from one local network to another. He is given other network credentials from the DHCP server, in which UTM is specified by the gateway, and if any activity on the part of the user is detected, the second session with authorization by MAC address will appear.

> If the user does not have access and can’t see the second session with authorization by MAC address, then most likely this could have happened due to the fact that the user's network credentials were not updated.
> Reset the old network credentials from the DHCP server and get new ones using the command:
> `ipconfig /release && ipconfig /renew`.

Configuring MAC Address Authorization for Network Printer and Other Network Devices

> Network printers and other network devices that need access to the internet must be authorized on UTM. Such devices can be called static and authorization by MAC address is perfect for them.

In order to authorize a network printer, you need to create a user for this printer manually or through **Netscan**.



User & Group

Username: Xerox

Login: xerox

Found in a group: Printers

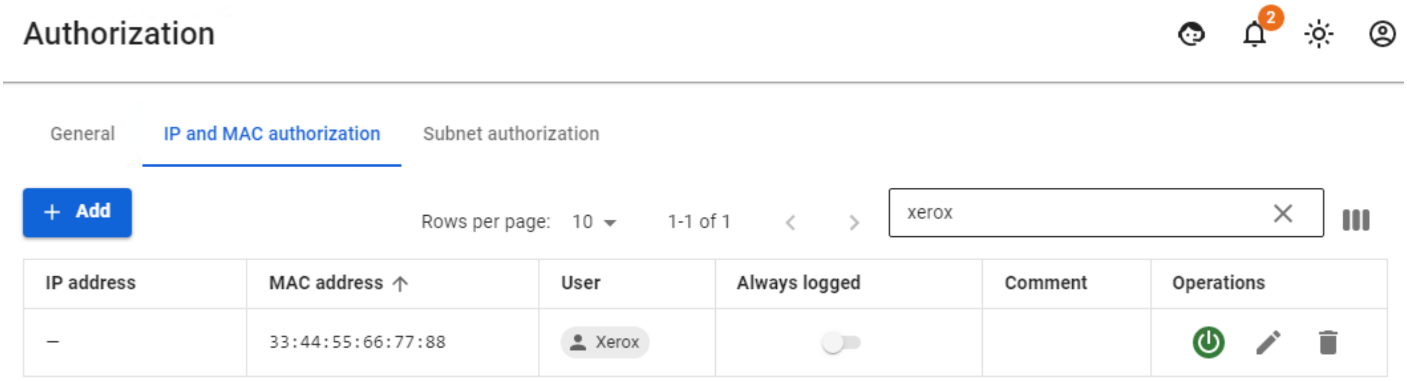
Operations

Additional settings

□ Deny access

□ Allow remote access via VPN

For a network printer, in **Users -> Authorization -> IP and MAC authorization you** need to create a rule **User <--> MAC address.**



IP address	MAC address ↑	User	Always logged	Comment	Operations
–	33:44:55:66:77:88	Xerox			

When detecting activity from a network printer or other device, its user will immediately appear in **Monitoring -> Authorized users.**

> In modern phones, there is an option for **MAC Randomization**. This option will interfere with phone authorization by MAC address. It is recommended to disable this option or use other types of authorization (for example, **web authorization**)

Revision #6
Created 22 August 2022 14:58:28 by Val Redman
Updated 12 October 2022 00:01:54 by Val Redman