User tree

User tree

In the SafeUTM management interface, users are displayed as a tree.

Users can be organized into trees. The group nesting level is not limited.
The user account tree is available in **Users -> User & Group**.

SafeUTM implements the principle of inheritance, which makes it easy to set and change parameters common for users, defining them for the parent group, for example, quotas or remote VPN access. The principle of inheritance is very convenient for performing management operations related to all users in the group.

An example of a user tree can be seen below:

The user's icon can be colored differently. The table below provides a description of each color of the user's icon:

| User Account Status	Description

🟢	The user has completed the authorization procedure and has been granted internet access.
🟠	Authorization restriction has been set in the **User Settings**.
⚫	The user has not completed the authorization procedure and has not been granted internet access.

User & Group

Creating, deleting, and moving user accounts.

General

To manage groups and accounts in the user tree, there are corresponding buttons on each group:

Symbol	Description
![create user icon]	Create user account
![create group icon]	Create group
![delete icon]	Delete user account or group

Creating User Account

To create an account in a certain group, click Create User Account in it. The control element symbols are illustrated in the table above.

The second way to create a user in a group is to select the designated group and click **Create User** in the right part of the window in the **General** tab.

Next, you will see a window for creating a user account, where you need to define a number of parameters. The form for creating a user account is shown below.

Login must be entered in lowercase Latin characters, for example, j.smith

Recommendations for creating password complexity: minimum length - 10 characters; use of lowercase and uppercase Latin characters; use of numbers and special characters. You can generate a password.

When you fill in the **Additional settings**, a corresponding rule will be created in the user card in the**IP and MAC authorization** tab and in the **Authorization -> IP and MAC authorization** section.

If this IP address or MAC address is used in DHCP server rules, then the **DHCP server** rule will be in priority.

For accounts imported from MS Active Directory (AD), password verification is carried out by means of AD. Active Directory user authorization is configured in the corresponding **section**.

You cannot create a user in the Active Directory group from SafeUTM. If you need to add an additional user to the Active Directory group, you must do so in the user tree on the domain controller.

It is impossible to view or restore the account password, only changing is allowed.

After you have entered all required parameters, click **Save**. An account will be created that will automatically get all the values of some parameters of the group in which it was created.

Creating Group

To create a group, you need to click on the corresponding control symbol to the right of the group name (you can create both a tree root group and a child group).

A window will open, in which you will need to type in the name of the new group and click **Save**. An example of adding a group can be seen below:

Mass Creation of Users with Authorization by IP

Mass creation of users for authorization by IP is possible. You can find out more in the **article** about this kind of authorization.

Alternatively, you can use **Netscan** to create them automatically when you try to access the internet.

Deleting Group or User Account

To delete a user account, select the user and click on the corresponding symbol. You can also select the user and click **Delete** in the **General** tab.

Deleting a group is done the same way.

Moving User Account or Group

To move a user account to another group, select this user in the **General** tab and find **Found in a group** field. From the drop-down list, select the group to move the user into and click **Save**.

Search

- **All**
  - **Accounting**
    - **Head**
      - Jane Smith
    - **Sales**
      - Dwight Schrute
      - Jim Halpert
      - Michael Scott
      - Pam Beesly
      - Ryan Howard
- **Developers**
  - George Johnson

General   Quota   IP and MAC authorization

Username
Jim Halpert

Login
halpert

Found in a group
Sales ▲

- All
- Accounting
- Head
- Sales
- Developers

Configuring Users

Configuring user account settings.

Categories

Users are configured in **Users -> User & Group**. To determine/edit the user account settings, select the account in the user tree by left-clicking on it. The parameters of the selected account will appear on the right side of the screen. All configurable parameters are divided into categories: **General**, **Quota**, **IP and MAC authorization**, and **Sessions**. If you want to change the parameters of all users in the group, select the corresponding group in the user tree.

General category

The section of main settings includes many parameters determining the user account status. The basic parameters are:

- **Username**. The name of the user for whom the account is being created, for example, John Smith. Maximum 128 characters.
- **Login**. The login is used to complete the authorization procedure in various SafeUTM services. The login must contain Latin lowercase letters, for example, j.smith. Maximum 32 characters.
- **Found in a group**. The group the user belongs to. You can use this field to move the user to another existing group.
- **Deny access**. Prohibit the user from being authenticated in the SafeUTM gateway. It means the user cannot use the internet, send an email, or access a personal account.

- **Allow remote access via VPN**. Allow connecting to the SafeUTM server via VPN from the internet.

General   Quota   IP and MAC authorization   Sessions

Username
Jim Halpert

Login
halpert

Found in a group
Sales   ▼

Operations

Change password

Delete

Additional settings

☐ Deny access

☐ Allow remote access via VPN

Save

For users exported from **Active Directory**, there is a corresponding line above the user settings. For such users, it is impossible to edit the name, login, or move them to another group in the **General** tab.

Quota category

This section allows you to view and increase the user quota in case of using traffic limits.

General   **Quota**   IP and MAC authorization   Sessions

⬤ Inherit quota from group

Quotas
Quota for Accounting   ▼

Management is carried out in the Quotas section

Quota information

Limit (MB) .... 5,000 MB per month

Remainder .... available 5,000 MB

The quota will be reset .... in about 1 month, 10/01/2022

Increase traffic for the current period (MB)   **Increase**

To restrict access to a user with an exceeded quota,
you must create appropriate rules.

To increase the quota, use the **Increase traffic for the current period** field.
Example: A user is assigned a quota of 1000 MB for a week (Monday to Sunday). By Thursday, the amount of traffic exceeded the value set by the quota. It is required to provide the user with additional traffic once.
To do this, enter the required value in the **Increase traffic for the current period** field and click **Increase**. The **Remaining** line will reflect all available traffic, taking into account the added one.

> You can find the information about how to set up traffic quotas in the **User Quotas** section.

IP and MAC Authorization category

This category contains authorization rules by IP and MAC created for a specific user in two sections:

- Users -> User & Group -> IP and MAC authorization

- Users -> **Authorization** -> **IP and MAC authorization**

The **IP and MAC authorization** rules also create a similar binding in the SafeUTM **DHCP server**. But if the same IP and MAC addresses are used in enabled DHCP server rules, then the DHCP server rules will be executed first.

Sessions category

Contains a table with information about all active user sessions:

When you click on "X" in the **Operations** column, UTM will terminate the user's session.

A similar table is located in the **Monitoring** -> **Authorized users** section.

Terminal Server Users

Used for remote work with the provision of a separate desktop for each user. Provides a service for the work of dozens and even hundreds of users.

Terminal Server Authorization

If the admin does not need the separate authorization of terminal server users, and the same access settings (content filtering and user firewall) can be applied to them, the server can be authenticated as a single user.

The best option is **authorization by IP address**.

Please note that when the number of users on the terminal server is large, it may be necessary to **increase the number of simultaneous sessions** from one address in advanced security settings.

Authorization of Terminal Server Users

Separate authorization of terminal server users (running under Windows Server 2008 R2 and Windows Server 2012 OS) is possible using **SSO (NTLM)**. In such a case server authorization by IP is not necessary.
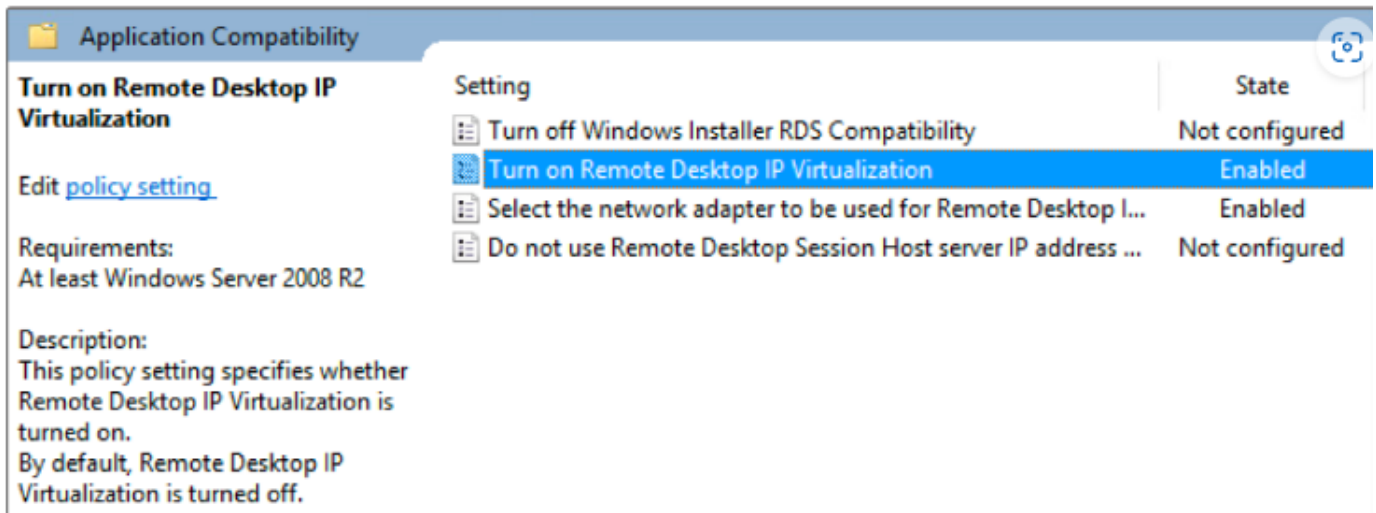
For separate authorization of terminal server users, **Remote Desktop IP Virtualization** must be configured on the terminal server, and user authorization via web authorization (SSO or NTLM) must be configured on the SafeUTM server. Authorization of terminal server users based on logs of the AD domain controller has not yet been implemented.

Configuring Remote Desktop IP Virtualization on Windows Server 2012

For the **Remote Desktop IP Virtualization** to work on one of Windows servers, the role of a DHCP server must be added (this function may not work correctly with other DHCP servers) and an IP address area for terminal server users must be allocated.

In **Group Policy Management Editor,** you need to navigate to **Computer Configuration –> Administrative Templates –>Windows Components -> Remote Desktop Services –> Remote Desktop Session Host –> App Compatibility**.

Enable the option **Turn on Remote Desktop IP Virtualization** in group policy with the option **Per Sessions**:

It is also recommended to enable the option **Do not use the IP address of the remote desktop session host server if the virtual IP address is unavailable**.

Use command `gpupdate /force` to update all policies.

You can check that the settings have changed using the following command in PowerShell:

`Get-WmiObject -Namespace root\cimv2\TerminalServices -query "select * from Win32_TSVirtualIP"`

Where values must be: `VirtualIPActive = 1` (virtualization on) and `VirtualIPMode=0` (for a session).