Manual MachineSelector

Version: 6.6.x

Publisher: Propius GmbH
Löscherstr. 18
01309 Dresden, Germany

Revision: 04

If you have any suggestions or proposals for improvement regarding the content and design of our manual, we would be pleased if you send us your suggestions to: support@propius.de

Table of Contents

1 Functionality

The *MachineSelector* (MS) is a web-based tool developed and managed by *Propius GmbH* with which both machine builders and operators can create, control and manage secure access (VPN connection) to their plants via a portal. The remote maintenance portal connects the user's PC with a selected machine network through routing and VPN technology. It comes with two internal VPN gateways to decrypt data coming from the user's PC and the machine network. Between them a dynamic firewall passes or blocks the traffic depending on user's access rights and machine selection. The machine networks are freely selectable, so not necessarily either all the same or all different. The VPN connections (machine and service tunnels) are linked in a dedicated manner via a VPN gateway.

The *MachineSelector* configures the unique assignment of a service to one or more machine tunnels. Through filters (access control list) defined by the administrator, the user (service technician) only sees the machines that they are allowed to access. This is controlled by the display and access management. In addition, the administrator can restrict IP address ranges of the machine network via the access lists for the user.

The administrator also generates all user and machine profiles that can be loaded as configurations on the service and machine side. All profiles receive a fixed, but editable certificate duration.

Furthermore, the MS also covers the operator scenario, i.e., plant operators can make parts of their plants defined by a controller visible to external suppliers/machine builders and thus permit their access on a time-controlled basis. The operator's administrator creates the access profiles for the suppliers. The access is controlled by a web-based user interface which can be accessed by any web browser. After logging in, the supplier can select the plants assigned to them and previously released by the controller, thus starting the routing of their client to the selected plant. They also see if a machine is online or not. The routing is interrupted by a manual stop of the connection or after expiration of the assigned time. If licensed, machine router profiles can be created and downloaded directly from the Web UI and installed plug & play.

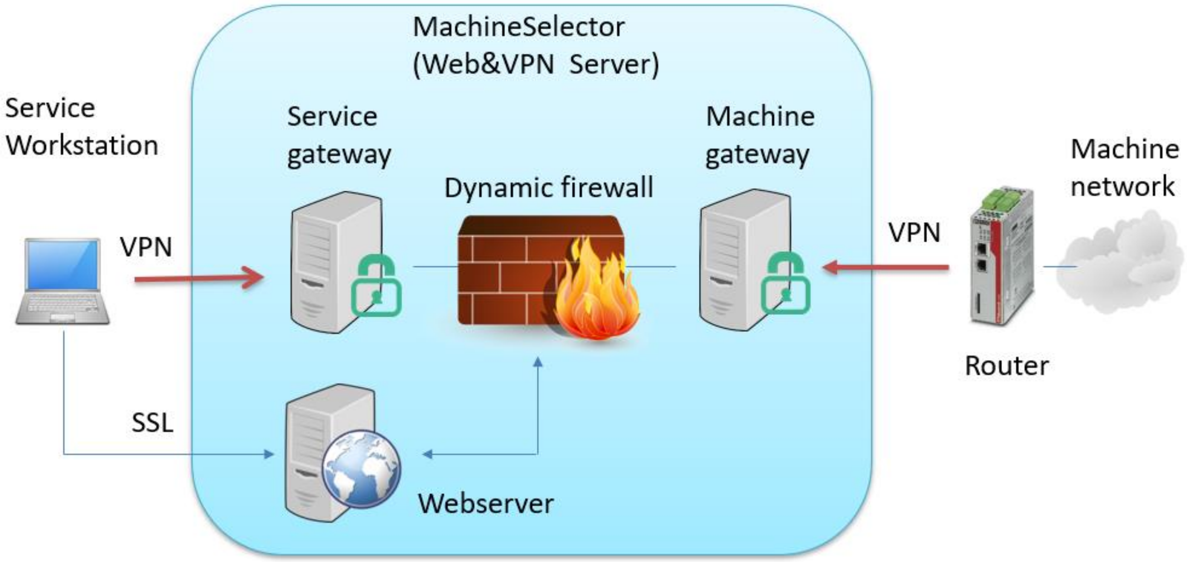


Figure 1: MachineSelector network diagram (overview)

2 Technical specifications (overview)

- Web UI
    - HTML5, *Javascript*
    - CSS3
    - Responsive design
    - Dark mode support

- Appliance
    - *Debian Linux OS*
    - SQL Database (*MariaDB*) with *adminer* interface
    - *Apache* Webserver, PHP extension, SSL, *Webmin*
    - User authentication by local database or LDAP connection
    - Two factor authentication (TOTP)
    - Build in PKI to create X.509 certificates for user and machine profiles
    - Dynamic routing and firewall system
    - Permission system to provide access permissions to machines and their components
    - Address translation to avoid routing conflicts

- VPN
    - *OpenVPN* server (Service and machine gateway)
    - *strongSwan IPSec* server (machine gateway)

- Installation
    - On premise (OVA, Hyper-V Image)
    - Cloud (*AWS*, *Azure*)

- Security
    - OWASP Top 10 certified
    - Daily security updates
    - Brute force protection
    - Modern encryption algorithms
    - Intrusion prevention system (*fail2ban*)
    - CVE communication of cybersecurity vulnerabilities

- Licenses
    - Machine amount
    - Profile generator for machine routers
    - Controller function to schedule timeframes for machine availability
    - License to connect an external *IPSec* machine gateway
    - License to operate an external HA *IPSec* machine gateway pair for redundancy

3 Usage scenarios

3.1 Using a build-in machine gateway

This hardware-less setup makes it possible to run the system on-premise as well as cloud hosted. Machine connections can be established with *IPSec* or *OpenVPN*. Service PCs encrypt data with *OpenVPN* since they are connected over unsecure networks.

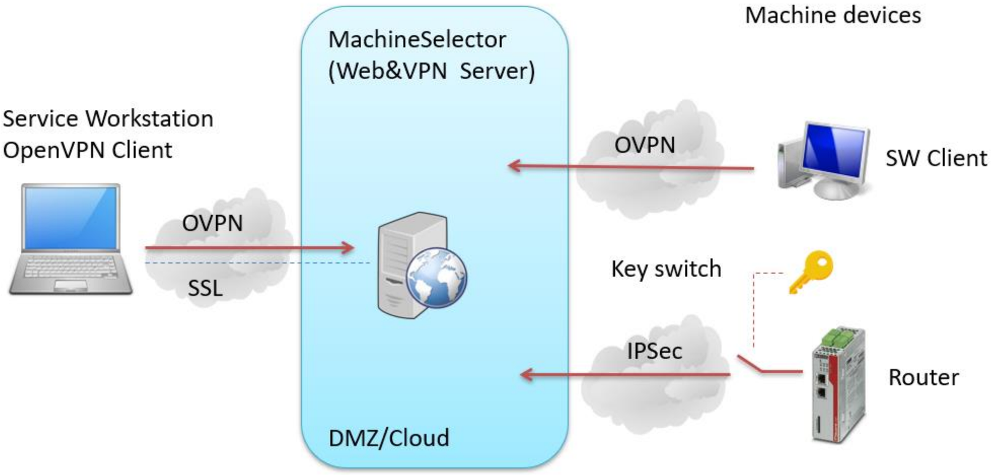


Figure 2: MachineSelector network diagram (built-in machine gateway)

3.2 Using an external machine gateway (licensed)

It is possible to attach an (already existing) external machine gateway (*PhoenixContact mGuard* series). The *MachineSelector* and this gateway must route the requests and answers. Since these packets are unencrypted, it is possible to attach other systems to log or process this data. Also, the *mGuard* TCP Encapsulation or *Pathfinder* technology can be used to establish the machine VPN connection.

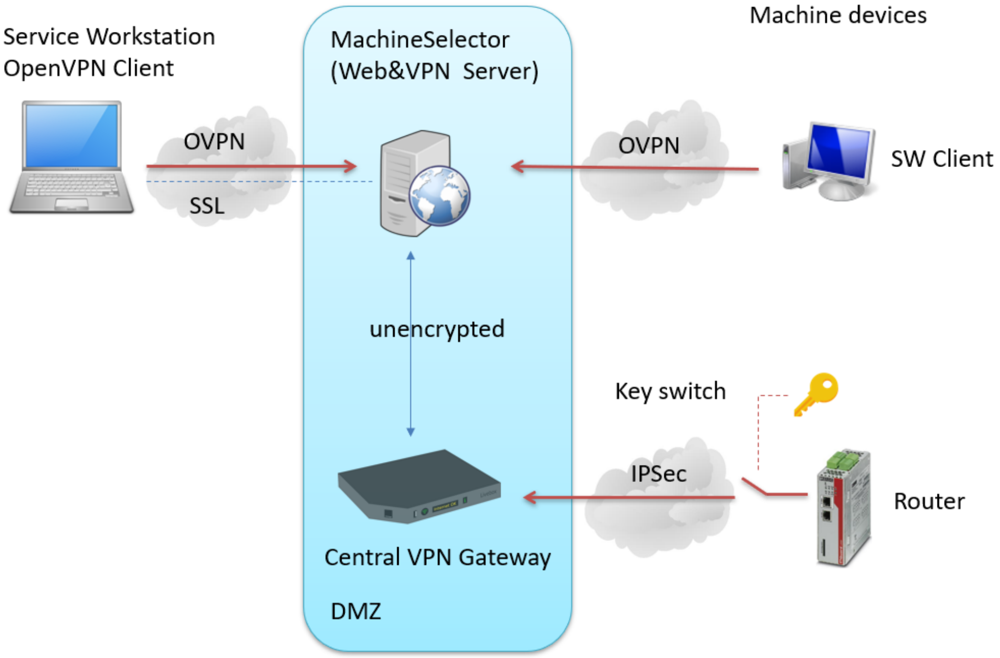


Figure 3: MachineSelector network diagram (external machine gateway)

3.3 Operate users without VPN

If the user is in the same environment as the *MachineSelector* and can route packets directly to it securely, there is no need to use a local VPN client. Packets must not be masqueraded while routed to the *MachineSelector*. This setup can also be used if already existing VPN clients connect the user's PC to the corporate network. The *MachineSelector* obtains the user's source IP address and masquerades it with a pre-configured virtual address which fits to the machine VPN connections.

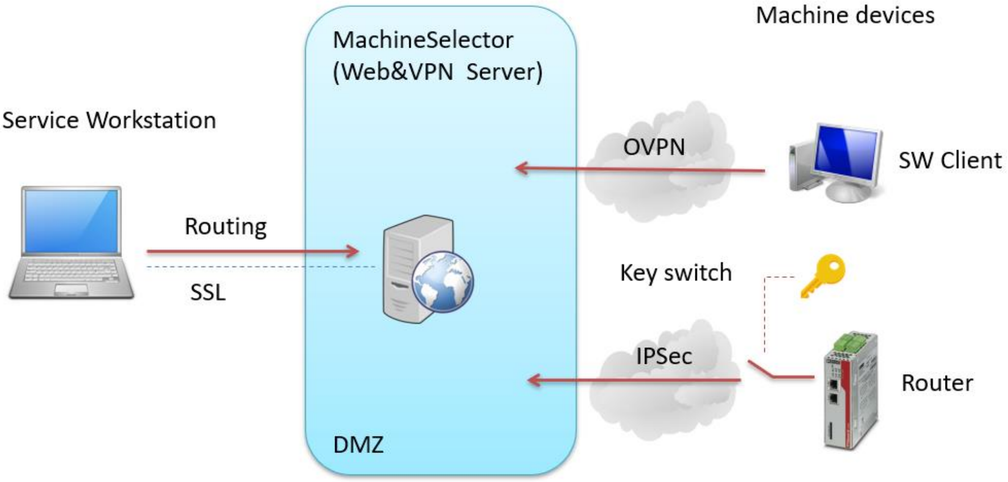


Figure 4: MachineSelector network diagram (user without VPV)

3.4 Packet translation

If the same network is used on multiple machines, it is necessary to configure unique networks in the machine VPN connection to avoid routing conflicts. To keep the user from working with those virtual networks, the *MachineSelector* is able to translate (1:1 NAT) the packets. The machine device has to turn it back into the real network. In this case it is suggested to use the NAT option while creating machines.

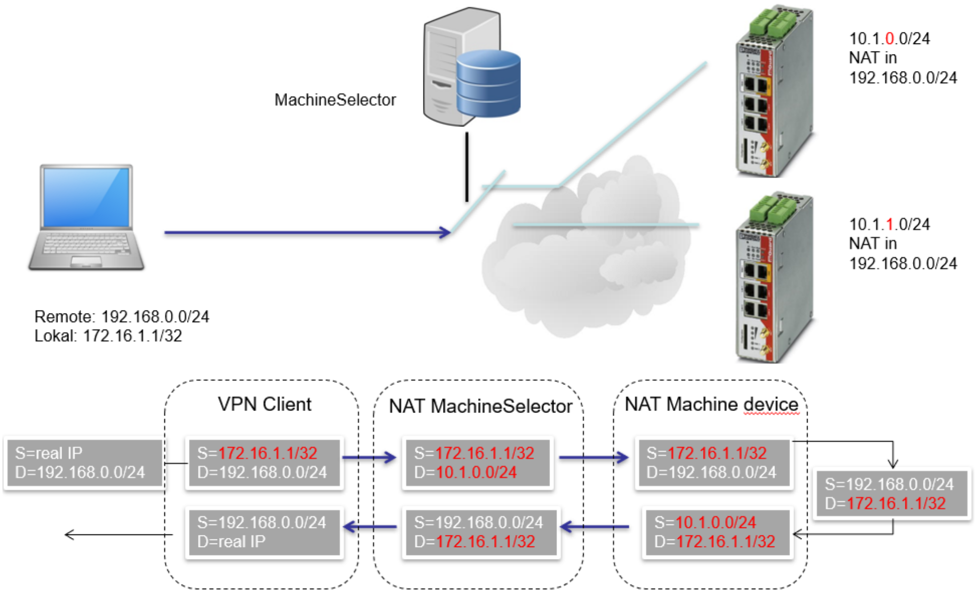


Figure 5: MachineSelector network diagram (packet translation)

4 License Models

4.1 Machine licenses

The total amount of machines must be licensed. 10 machines are included in the base version. If the machine limit is exceeded, it is still possible to add additional machines, but the user(s) are not allowed to switch to it. This limitation works in a chronological order. Machine licenses can be purchased as cumulative packs. Available packs are 10, 50, 100 and 250 additional machines.

4.2 External *IPSec* gateway license (SW-1013)

If desired, it is possible to operate an external machine gateway. For this application *PhoenixContact mGuard* products are recommended. A license must be purchase first.

4.3 External *IPSec* gateway redundancy license (SW-1003)

This license enables the *MachineSelector* to support the *mGuard* firewall and VPN redundancy function (see product 2702193). Additionally, SW-1013 must be purchased. Two external *mGuard* devices are required.

4.4 Profile generator license (SW-1004)

This license enables the profile generator function (see 8.2.2) to create and export configuration profiles for machine router devices. This license is already included in the *MS* bundle (SW-1011).

4.5 Controller license (SW-1014)

This license enables the controller user role (see 10). Controllers can schedule time frames for machine availability. This can be used in a machine operator setup.

5 Features

5.1 Roles

5.1.1 Administrator

An administrator is able to perform various system tasks using the *Machine Selector* (MS). The administrator(s) plan, install and configurate the system infrastructure. Every administrator is also a user at the same time. The desired role can be selected via the user profile by hovering above the name in the top right corner and selecting *User page* or *Admin page* (see 11). An administrator is able but not limited to create and delete other users (see 7.1). This includes administrators, controllers (licensed) and regular users. The administrator is also able to create and delete machines (see 8.1) as well as starting a remote maintenance to the system for support inquiries to *Propius GmbH* (see 11.6). The administrator can also manage access control lists (see 7.3), machine tags (see 8.3) and permission groups (see 8.4). Different logs can also be viewed by the administrator (see 12).

5.1.2 Controller (licensed)

The controller role requires a separate license that can be purchased. The controller is able to grand access to certain machines to specific users. The controller can also schedule (time) these accesses, giving a user access to a certain machine for a set period of time (see 10.2). This feature can be utilized for granting a specific customer access to a specific number of machines for a specific time frame. After the time expires, the customer will not be able to access the machines again for as long as the controller grants access again.

5.1.3 User

Users are able to perform various tasks within the target device using the *MS*. The user is only able to access a specific machine after either the controller or the administrator has granted access. Any machine that cannot be accessed by the user will not be visible for the user. It is possible for the user to filter machines via the machine tags and leave a comment when connecting to a machine.

5.2 Access control list (ACL)

An access control list (ACL) a set of rules that grand or deny network users and devices access to certain network areas. It works like a filter that denies all access to network devices that are outside of this area for the network user. As an administrator it is possible to specify the user(s) that will have access to specific network areas, in this case specific target devices (machines) (see 7.3). If an *OVPN* client is utilized, the ACL also pushes the IP address(es) and/or network(s) to the client. An ACL contains at least one IP address or network, specifying the area that can be accessed through this ACL. It can also contain multiple IP addresses or networks. Large ACL network areas might lead to routing errors on the user-side. The ACL is assigned to the network user(s). The default ACL will grand the user access to all target devices.

5.3 User groups

User can be collected in a user group. It is not possible to add a user with the controller role into a user group. User groups are used to simplify the controller's operation. The controller is able to grand permission to a group of users all at once instead of having to add single users manually. This feature can be helpful in a scenario in which it is unknown which specific technician will need access to a certain machine. With the user group all users within the group will have access for the specified time frame.

5.4 Tags

A tag can be assigned to a target device (machine) and creates a distinctive characteristic that can be filtered for. Up to three tags can be assigned to a single machine (see 8.1). Especially for networks with a large number of target devices this method provides a simple solution for basic filtering. Tags are linked by a logic AND. Different values can be assigned to a single tag. For example, the tags can be named *country*, *location* and *manager*. It is now possible to assign one machine the country tag *Example_country_1* and another machine the country tag *Example_country_2*. Additionally, it is possible to assign the location tag *Example_town_1* to the first machine and *Example_town_2* to the second one. The values that can be added to one specific tag are unlimited.

5.5 Permission groups

Permission groups can be created and assigned to certain target devices (see 8.1). These groups include at least one machine. Assigning a user to a specific group allows the user to view all affiliated machines. Machines not assigned to this permission group will be hidden for the user(s). If the user is not assigned any permission group, the user/controller will be able to view all machines. Machines can be added to and deleted from the group without having to assign the group again (see 8.5). Permission groups can be filtered via the tags. Tags can also simplify the creation of permission groups.

5.6 Connection via *OpenVPN* client (additional software)

If the network infrastructure is designed to utilize the internet for a secure VPN connection to the target device via the *MS*, the *OpenVPN* (*OVPN*) client must be installed. The *OPVN* performs the routing from the user’s local IP address to the service network automatically (see 7.2.2).

Please follow the instructions provided by the *OVPN* website. (https://openvpn.net/)

5.7 Connection without usage of VPN

If the connection to machines utilizes a private network, it is not required to install the *OVPN* client. In this case the user’s local IP address is translated (NAT; network address translation) into an address compatible with service network. The connection is established via a physical private network (for example: company network). It is required to manually add a suitable IP address to the *MS* when creating a user and a route to the local routing table. If the local source device is located within the same subnetwork as the *MS* and the device utilizes the *Windows* operating system, the route can be added via a *Windows* command. Otherwise, the route has to be installed on the central routing equipment (gateway/next hop). If the source device and the *MS* do not share the same subnetwork, the routing needs to go through a gateway (see 7.1). Please note: no masquerading must be configured. Each user must publish a unique IP address to the *MS*.

5.8 Two-factor authentication (2FA) (additional software)

In order to utilize the two-factor authentication (2FA) feature when creating a user (see 7.1), it is necessary to install a TOTP (time-based one-time password) application on a smart mobile device (smart phone). Suitable applications include *Authy*, *Google Authenticator* and *Microsoft Authenticator*. Other applications may be utilized as well. The 2FA feature increases the security of the user's account.

6 Quick Start

In order to utilize the *MachineSelector* (MS) right away, follow the steps below. Detailed descriptions of the intermediate steps will be shown in the following chapters.

(1) Install the *MachineSelector*. (See installation manual)

(2) If you are trying to reach a network through the internet, install the *OpenVPN* client (https://openvpn.net/community-downloads/). If you are utilizing the *MS* on premise, it is possible to run the *MS* without the *OVPN* client.

(3) Log into the MS via the login credentials you have assigned during the installation setup.

(4) Create user(s) as an administrator (see 7.1). If you are utilizing the *MS* on premise and decided against the *OVPN* client, each user needs an individual IP address and a manual routing.

(5) If you are trying to reach a network through the internet, download the *OpenVPN* user profile (see 7.2.2) and import it into the corresponding *OpenVPN* client. If you are utilizing the *MS* on premise and decided against the *OVPN* client, skip this step.

(6) Create machine(s) as an administrator (see 8.1).

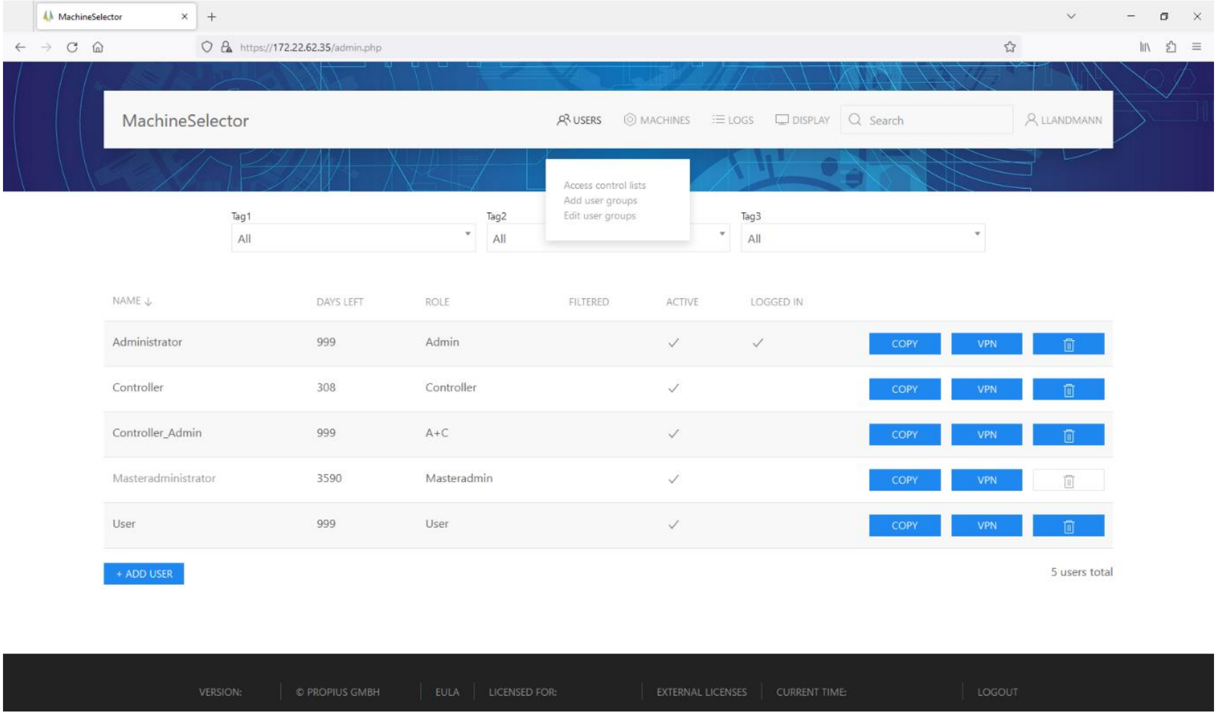
(7) If the controller license is purchased, set the machine to inactive in order for the controller to be able to schedule the machine (see 10.2). If there is no controller, all active machines can be accessed by the users. All inactive machines cannot be accessed by the users.

(8) If the corresponding license is purchased, generate a machine VPN profile (see 8.2.2) and import it into the target device (machine).

(9) The controller is now able to schedule the machine (see 10.2.3).

(10)The user is able to establish a VPN tunnel to the corresponding machine utilizing the *MachineSelector* and the *OpenVPN* client as long as the machine is physically online.

7 USERS overview (Administrator)

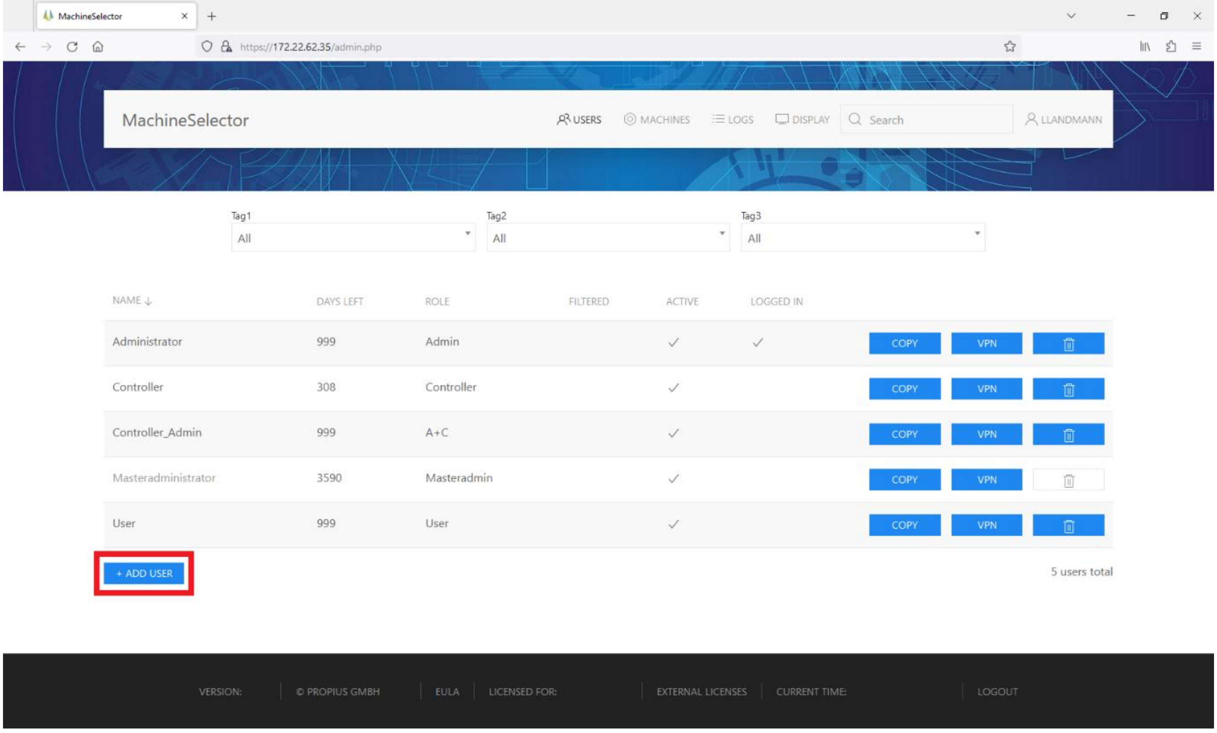


NAME ↓	DAYS LEFT	ROLE	FILTERED	ACTIVE	LOGGED IN
Administrator	999	Admin		✓	✓
Controller	308	Controller		✓	
Controller_Admin	999	A+C		✓	
Masteradministrator	3590	Masteradmin		✓	
User	999	User		✓	

5 users total

Figure 6: USERS (overview)

7.1 Create Administrators/Controller/Users

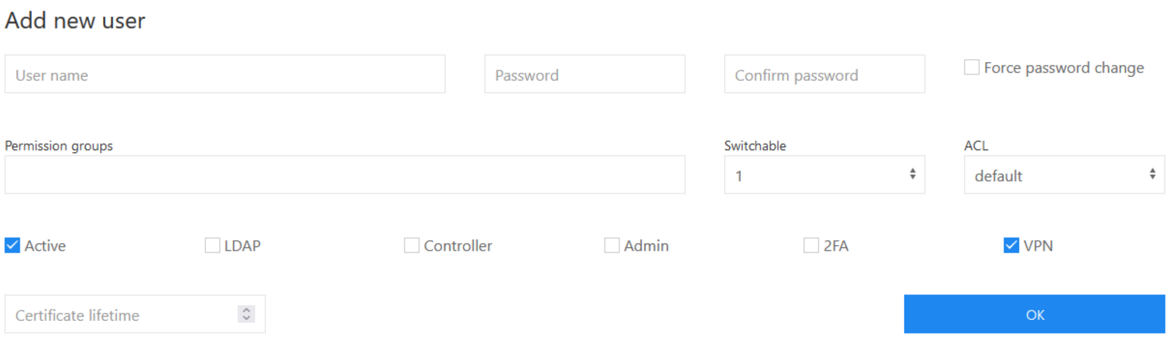


NAME ↓	DAYS LEFT	ROLE	FILTERED	ACTIVE	LOGGED IN
Administrator	999	Admin		✓	✓
Controller	308	Controller		✓	
Controller_Admin	999	A+C		✓	
Masteradministrator	3590	Masteradmin		✓	
User	999	User		✓	

5 users total

Figure 7: +ADD USER

To create a new administrator, controller or user, the masteradministrator initially has to select *+ ADD USER* on the *USER* overview page. After this initial setup, regular administrators are able to create additional administrator(s) as well as controller and user(s).



Add new user

User name | Password | Confirm password | ☐ Force password change

Permission groups

Switchable: 1

ACL: default

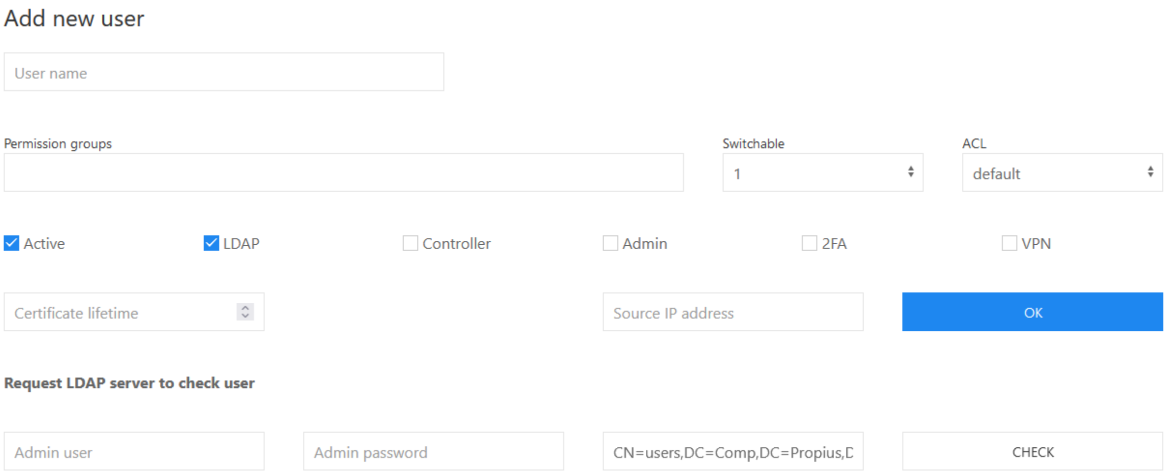
☑ Active ☐ LDAP ☐ Controller ☐ Admin ☐ 2FA ☑ VPN

Certificate lifetime

Figure 8: Add new user (default window)

- The administrator assigns the user's name and password. When the box *Force password change* is checked, the user is obligated to change the password upon the next login. This feature ensures that the user does not continue to use the assigned password. The old password cannot be reused. (Figure 8)
- The *Certificate lifetime* specifies the duration the user's *OVPN* connection will work. After the lifetime expires, the user cannot access the target device (machine) via the *MS*. The user's ability to log in will not be affected. (Figure 8)
- The administrator assigns the user one or more *Permission groups* (see 5.5). If not assigned any groups, the user will be able to access all permission groups available. (Figure 8)
- Up to 10 targets are switchable by the user at the same time, if the networks differentiate. The targets can be different machines. The administrator determines how many targets the user can switch at the same time. (Figure 8)
- The administrator specifies which *Access control list* (ACL) (see 5.2) will be assigned to the user. The user is not able to access network components outside of the ACL's restrictions. The *default* option grands the user access to defined network components (specified in the *default ACL*) of the selected machine(s). (Figure 8)
- The administrator is able to deactivate existing users via the *Active* box. The box needs to be checked if the user is supposed to be productive right away. Removing the checkmark deactivates the user who then cannot log into the *MS*. (Figure 8)
- Is the *LDAP* box checked, the user will be able to log into the *MS* using the *Windows* login. When selecting this feature, the password allocation will be hidden. The login requires the *MS* username to match the *AD* (*Active Directory*) username (*Windows* user with read rights) and the corresponding *AD* password. It is possible to verify the login before assigning this feature to a user. The *Admin user* field and the *Admin password* field need to be filled with the corresponding credentials. The field on the right side can be filled with the corresponding search path. The access will be verified by selecting *CHECK*. (Figure 9)
- The administrator is able to assign the user profile the roll of an *Administrator* by checking the *Admin* checkbox. Assigning the roll of a *Controller* is also possible. Additionally, *Controller(s)* can also be granted administrator rights by selecting both checkboxes. If the boxes remain blank, the created profile assumes the role of a regular *User*. (Figure 8)

- *Two factor authentication* (2FA) is used for additionally securing the user's login. TOTP (time-based one-time password) applications are being utilized for generating the second factor on the smart phone (see 5.8). (Figure 8)
- Checking the *VPN* box or leaving it blank depends on the infrastructure in which the *MS* is to be operated. If the user utilizes a VPN tunnel (*OVPN*) (see 5.6) to connect to the service network, the box needs to be checked. If the user utilizes a routing of the target network to the *MS*, the checkbox needs to be left blank. In this case the administrator is obligated to enter a unique virtual source (sender) IP address (address from the service network range) into the *Source IP address*-field. Additionally, a route to the desired machine network must be added manually on the local service device. (Figure 9)



Add new user

User name

Permission groups

Switchable: 1

ACL: default

☑ Active ☑ LDAP □ Controller □ Admin □ 2FA □ VPN

Certificate lifetime

Source IP address

OK

Request LDAP server to check user

Admin user

Admin password

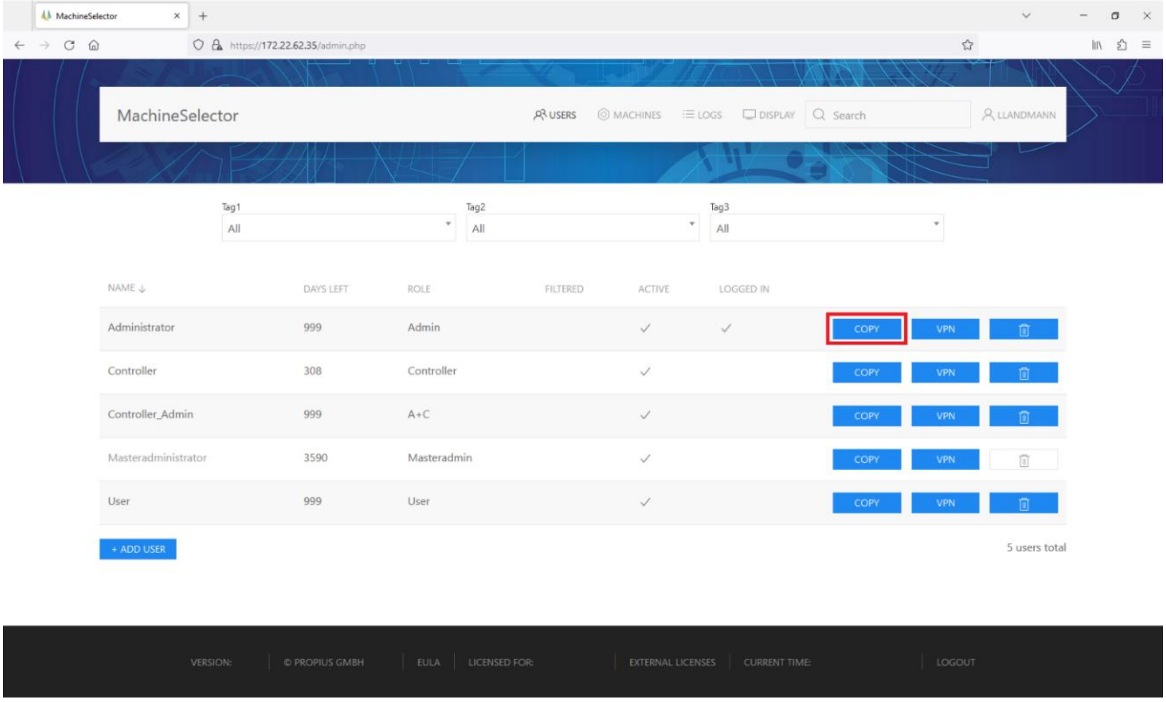
CN=users,DC=Comp,DC=Propius,D

CHECK

Figure 9: Add new user (LDAP enabled; VPN disabled)

7.2 Additional Settings

7.2.1 Copy



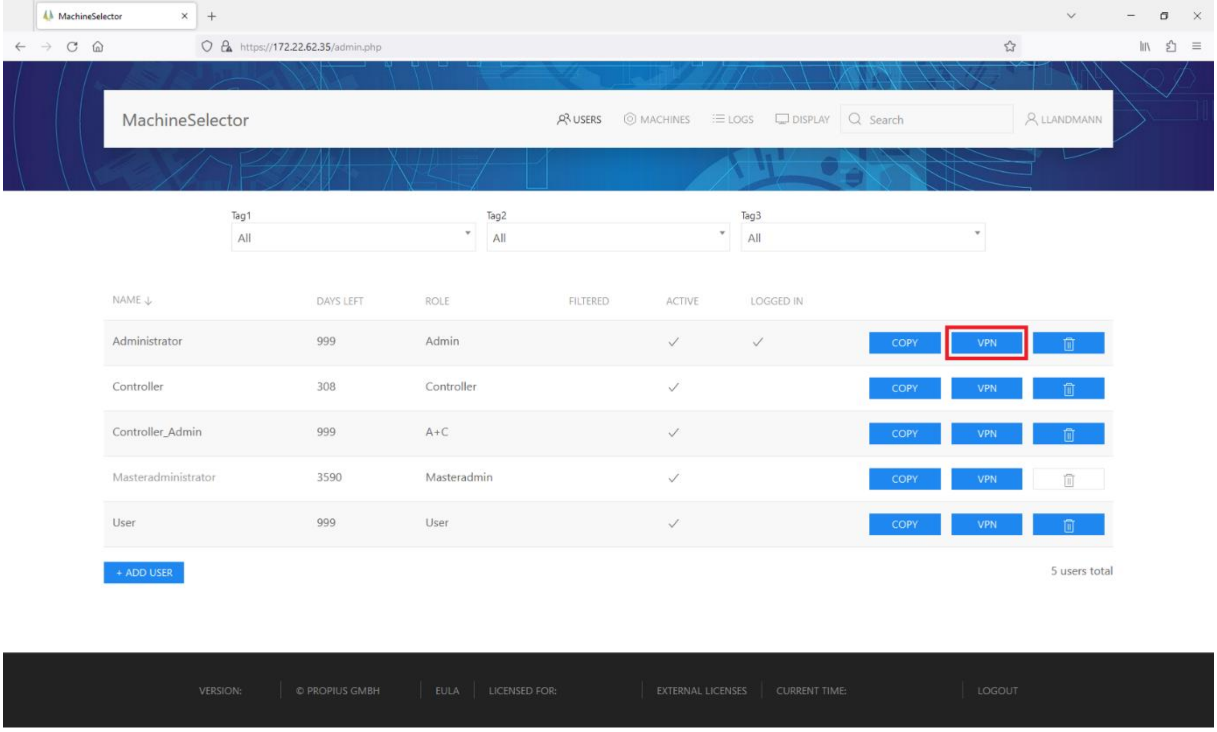
Tag1: All
Tag2: All
Tag3: All

NAME ↓	DAYS LEFT	ROLE	FILTERED	ACTIVE	LOGGED IN			
Administrator	999	Admin		✓	✓	COPY	VPN	🗑
Controller	308	Controller		✓		COPY	VPN	🗑
Controller_Admin	999	A+C		✓		COPY	VPN	🗑
Masteradministrator	3590	Masteradmin		✓		COPY	VPN	🗑
User	999	User		✓		COPY	VPN	🗑

Figure 10: COPY USER

The *COPY* button allows the administrator to duplicate a user. All settings, except for the password, will be carried over to the new user (see 7.1).

7.2.2 VPN

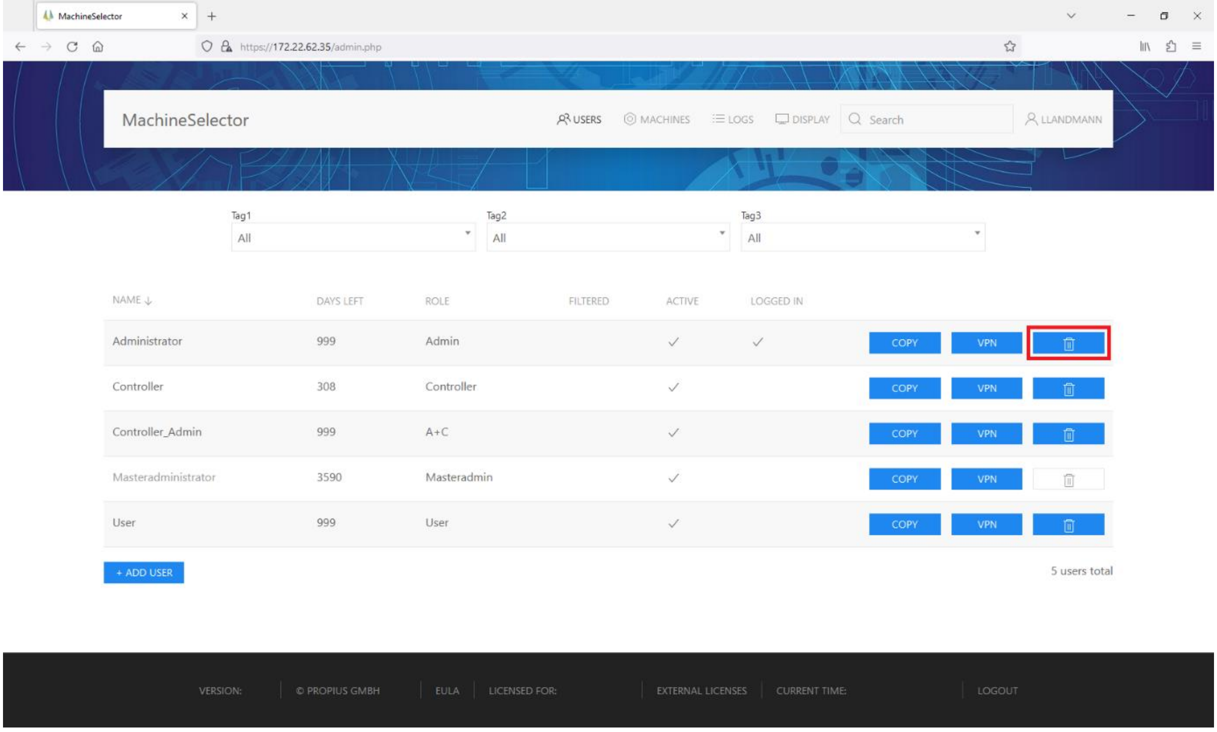


NAME ↓	DAYS LEFT	ROLE	FILTERED	ACTIVE	LOGGED IN			
Administrator	999	Admin		✓	✓	COPY	VPN	🗑
Controller	308	Controller		✓		COPY	VPN	🗑
Controller_Admin	999	A+C		✓		COPY	VPN	🗑
Masteradministrator	3590	Masteradmin		✓		COPY	VPN	🗑
User	999	User		✓		COPY	VPN	🗑

Figure 11: VPN USER profile

The *VPN* button allows the administrator to download and optionally set a password for the user's individual *OpenVPN* certificate (profile). The password will be reset every time the administrator requests the profile again. The profile can also be downloaded by the user via the *ACCOUNT menu* (see 11.4) by hovering above the user's name and selecting *Download VPN profile*. If the administrator does not set a password, the user will not have to enter a password when connecting to the *MS* via the *OPVN* client. If the password is set, the user will have to enter it every time a connection to the *MS* is established via the *OPVN* client. Please note: if the administrator re-downloads the user's profile, the old certificate will be revoked. This prevents the user to connect to the *MS*.

7.2.3 Delete User



Tag1: All
Tag2: All
Tag3: All

NAME ↓	DAYS LEFT	ROLE	FILTERED	ACTIVE	LOGGED IN			
Administrator	999	Admin		✓	✓	COPY	VPN	🗑
Controller	308	Controller		✓		COPY	VPN	🗑
Controller_Admin	999	A+C		✓		COPY	VPN	🗑
Masteradministrator	3590	Masteradmin		✓		COPY	VPN	🗑
User	999	User		✓		COPY	VPN	🗑

+ ADD USER

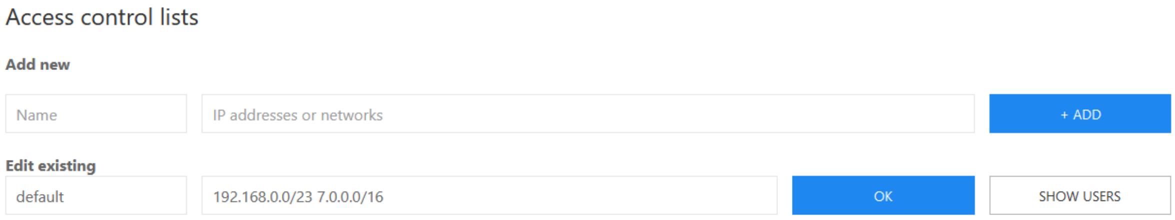
5 users total

Figure 12: DELETE USER

In case a user is no longer needed, it is possible to delete the user. To delete the user, the administrator selects the trashcan icon next to the desired user on the *USERS* overview page. The certificate will be revoked and no *OVPN* connections will be possible anymore. A deleted user cannot be recovered.

7.3 Access control lists

In order to edit the access control list (ACL), the administrator navigates to the *Access control lists* tab by hovering above the *USERS* button. (Figure 6)


Access control lists

Add new

Name | IP addresses or networks | + ADD

Edit existing

default | 192.168.0.0/23 7.0.0.0/16 | OK | SHOW USERS

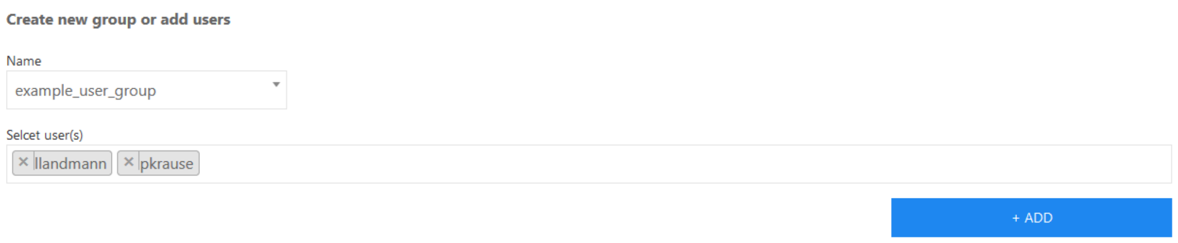
Figure 13: Access control list window

- It is possible to add a new ACL by choosing a name and at least one IP address/network in CIDR (Classless Inter-Domain Routing) notation and confirming by selecting the *+ ADD* button. The IP address(es) and/or network(s) need to be separated by whitespaces. (Figure 13)
- Existing ACLs can be renamed and/or given new IP addresses and/or networks. Within this menu it is also possible to filter for users with certain ACLs. (Figure 13)

7.4 User group

7.4.1 Add user group

In order to add a new user group, the administrator navigates to the *Add user groups* tab by hovering above the *USERS* button. (Figure 6)



Create new group or add users

Name

example_user_group

Selcet user(s)

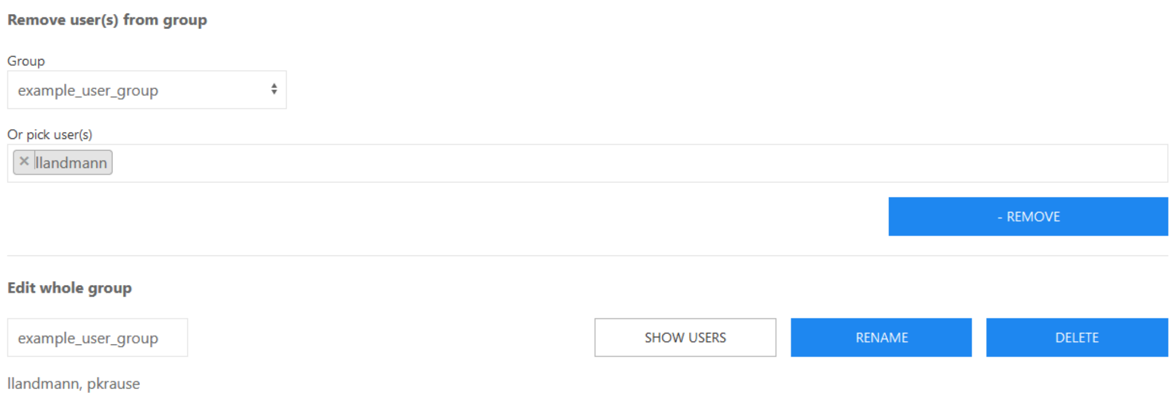
× llandmann × pkrause

Figure 14: Add user group window

- A new user group is created by selecting the *Name* field and selecting the corresponding user(s) from the list via the *Select user(s) field*. (Figure 14)

7.4.2 Edit user group

In order to edit a user group, the administrator navigates to the *Edit user group* tab by hovering above the *USER* button. (Figure 6) This tab allows for the removal of users from groups and to edit the group itself.



Remove user(s) from group

Group

example_user_group

Or pick user(s)

× llandmann

Edit whole group

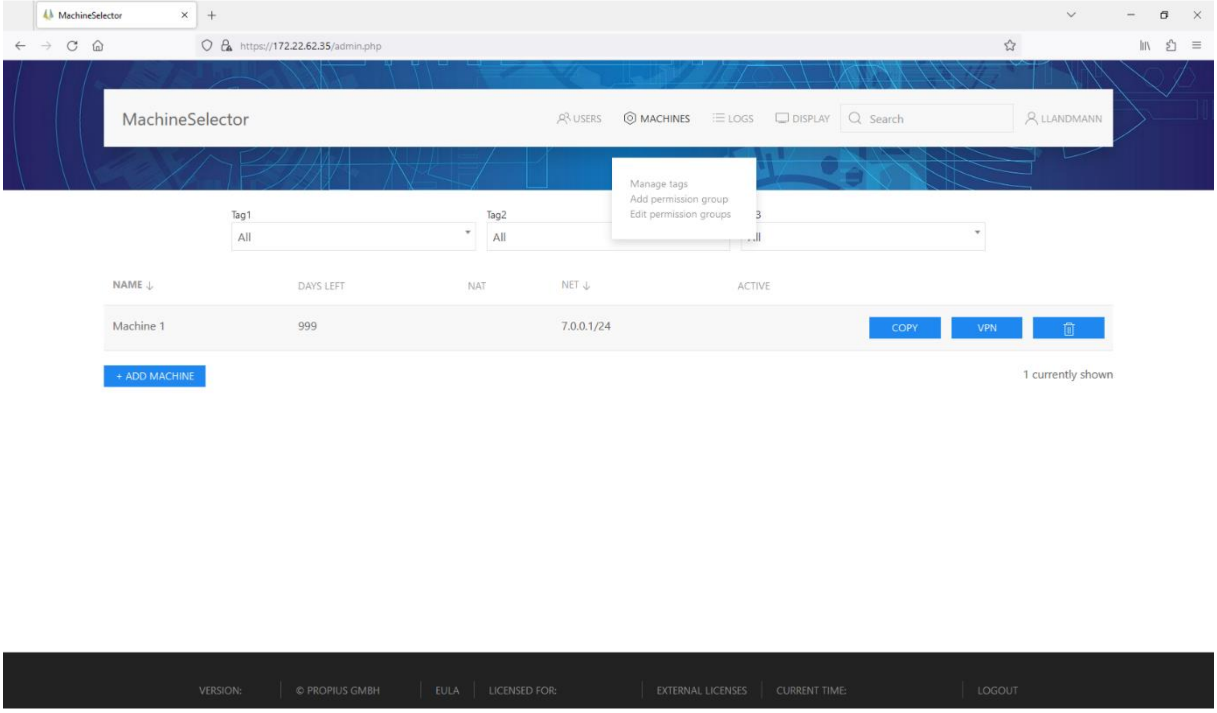
example_user_group

llandmann, pkrause

Figure 15: Edit user group window

- It is possible to remove certain users from a group by selecting an existing group via the *Group* field followed by picking specific users via the *Or pick user(s)* field. (Figure 15)
- It is possible to rename and delete an entire group by selecting the corresponding buttons. *SHOW USERS* shows all users who are member of this group. (Figure 15)

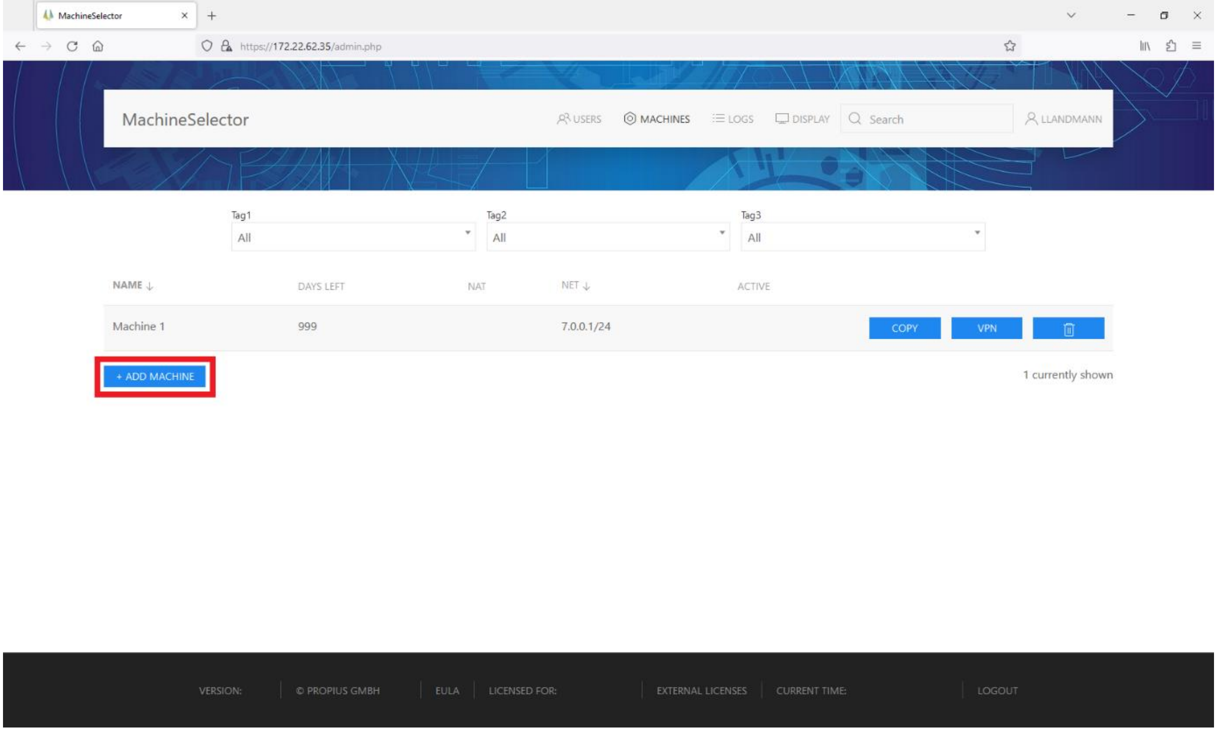
8 MACHINES overview (Administrator)



NAME ↓	DAYS LEFT	NAT	NET ↓	ACTIVE			
Machine 1	999		7.0.0.1/24		COPY	VPN	🗑

Figure 16: MACHINES (overview)

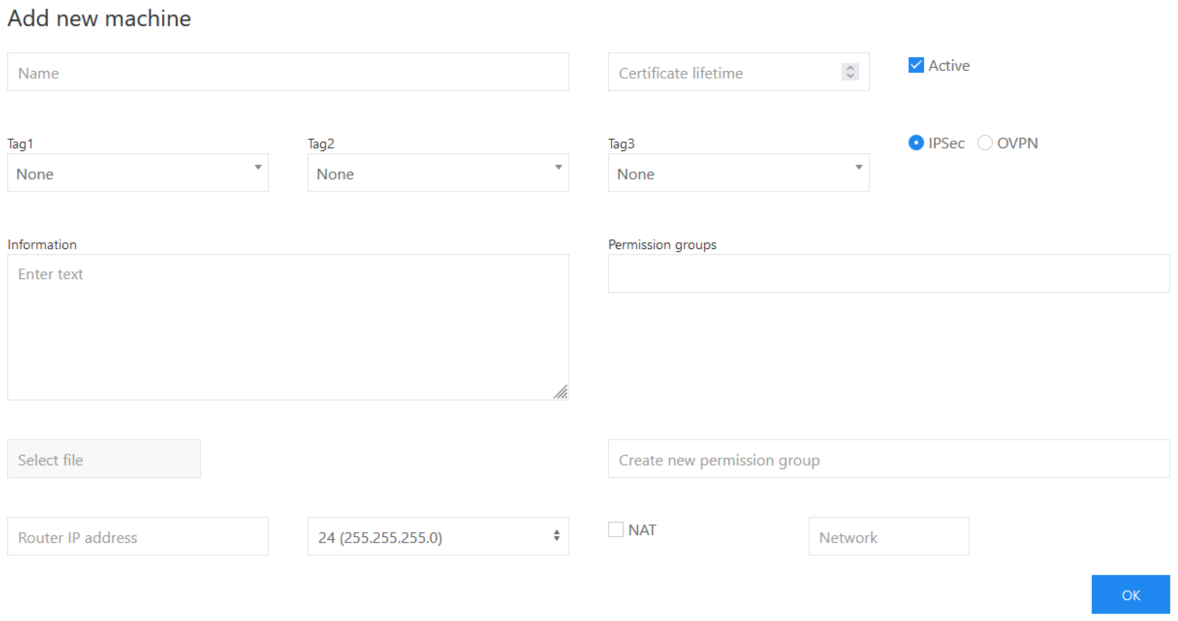
8.1 Create Machines



NAME ↓	DAYS LEFT	NAT	NET ↓	ACTIVE			
Machine 1	999		7.0.0.1/24		COPY	VPN	🗑

Figure 17: +ADD MACHINE

To create a new machine, the administrator needs to select *+ ADD MACHINE* on the *MACHINES* overview page.



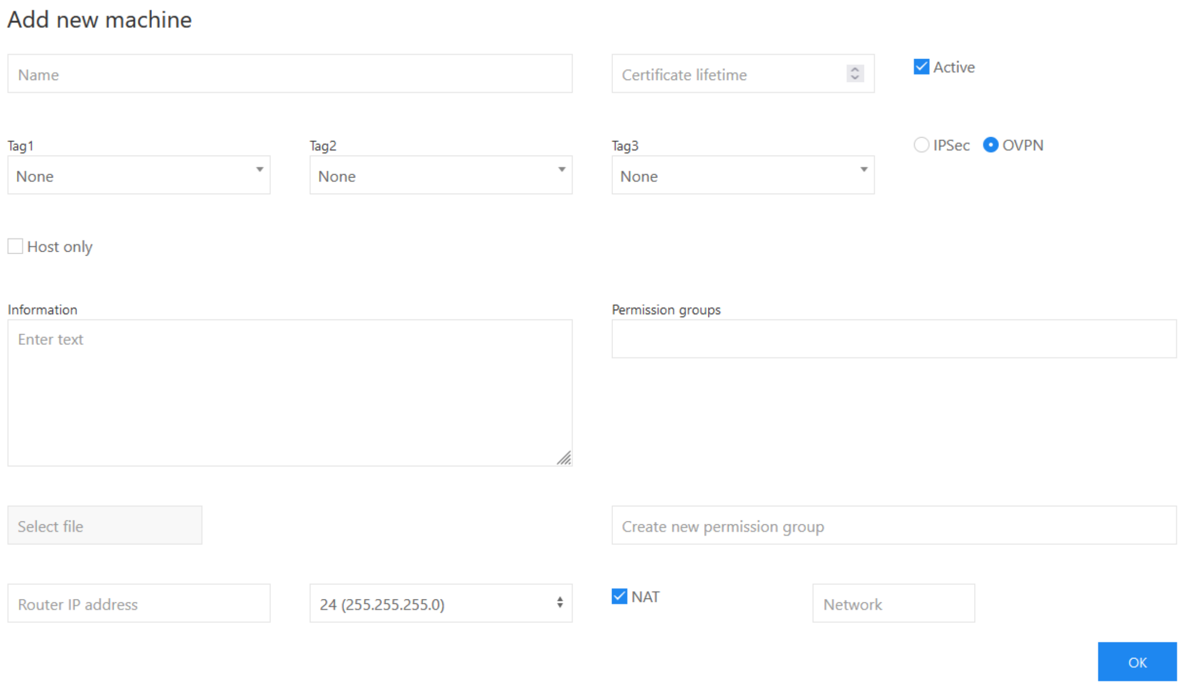
Add new machine

Name		Certificate lifetime	☑ Active
Tag1: None	Tag2: None	Tag3: None	● IPSec ○ OVPN
Information: Enter text		Permission groups	
Select file		Create new permission group	
Router IP address	24 (255.255.255.0)	□ NAT	Network

Figure 18: Add new machine (default window)

- The administrator assigns a *name* and a *certificate lifetime* to the machine. After this step, there are two different possible scenarios:
  - Setup without controller: If the machine is not needed right away, it is possible to deactivate the machine by unchecking the *Active* box. If checked all users with the corresponding permission group or without any permission group are able to see the machine. Removing the checkmark in the *Active* box hides the machine for all users. This option can be changed later.
  - Setup with controller: Unchecking the Active box enables the controller to set time frames for (schedule) the machine in which the machine can be accessed by the users. In this case the checkmark is set automatically by the *MS* according to the controller's input. Is the checkmark set by the administrator, it is not possible for the controller to schedule the machine. (Figure 18)
- It is possible to assign up to three *Tags* to the machine. Via the *tags* it is possible to filter the machines on the *MACHINES* overview page (see 5.4). To create a new tag, the creator fills the unfolded box with a valid tag and confirms the input. (Figure 18)
- When creating a machine, the administrator choses between *IPSec* or *OVPN*. The two options differ in the VPN protocols that are being utilized and ultimately in the VPN clients used. The *MS* will create different VPN configurations according to this option. When selecting the *OPVN* option (see Figure 19) the creator can checkmark the *Host only* option. This creates a VPN configuration that is suitable for *OVPN* software clients on the machine end of the VPN tunnel. Unchecking this box (see Figure 18) creates a configuration that is suitable for multiple IP addresses (router).
- The information that is entered in the *Information* text box will appear when selecting the machine's name on different overview pages. (Figure 18)
- Not selecting any *permission group(s)* will result in the machine being able to access all existing permission groups. (Figure 18)

- When creating a machine it is possible to additionally upload files that can be used to further identify or share information about the machine. These files will be shown when selecting the machine's name on multiple overview pages. Supported are all file types that are displayable by a regular web browser. (.gif, .jpeg, .pdf and .png) (Figure 18)
- It is possible to create a new permission group (see 5.5) via the *Add new machine* tab (Figure 18)
- The administrator needs to assign a *LAN IP address* and a *LAN netmask* to the machine. Checking the *NAT* checkbox allows the LAN IP address to differ from the VPN tunnel address. (Figure 19)



Add new machine

Name

Certificate lifetime

☑ Active

Tag1: None

Tag2: None

Tag3: None

○ IPSec ● OVPN

□ Host only

Information: Enter text

Permission groups

Select file

Create new permission group

Router IP address

24 (255.255.255.0)

☑ NAT

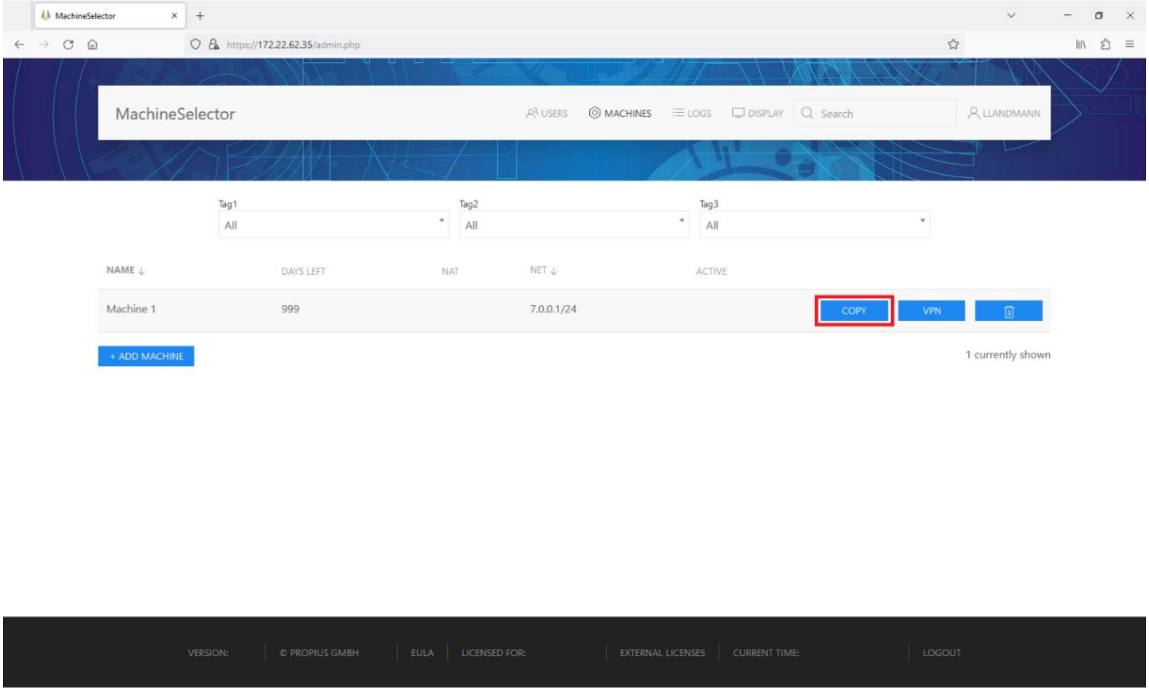
Network

OK

Figure 19: Add new machine (OVPN enabled; NAT enabled)

8.2 Additional Settings

8.2.1 Copy



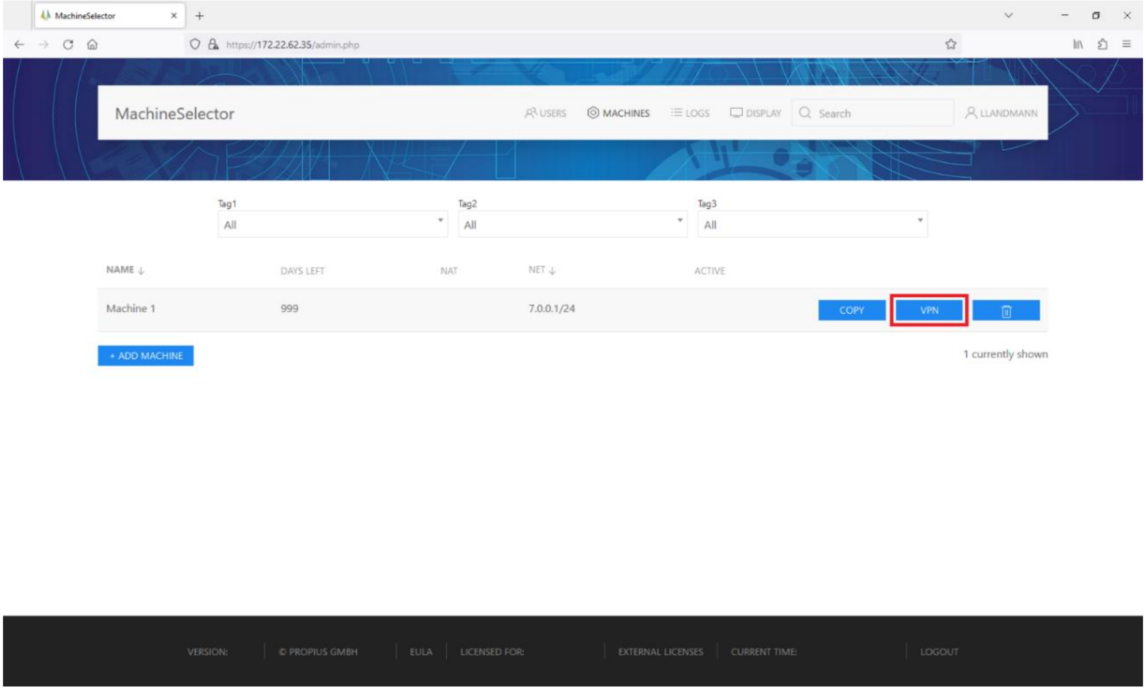
Tag1: All
Tag2: All
Tag3: All

NAME ↓	DAYS LEFT	NAT	NET ↓	ACTIVE
Machine 1	999		7.0.0.1/24	

Figure 20: COPY MACHINE

The button *COPY* duplicates the selected machine. All settings, except for the IP address, will be copied into the editor of the new machine. This feature minimizes the risk of false information input when creating similar machines.

8.2.2 VPN (licensed)



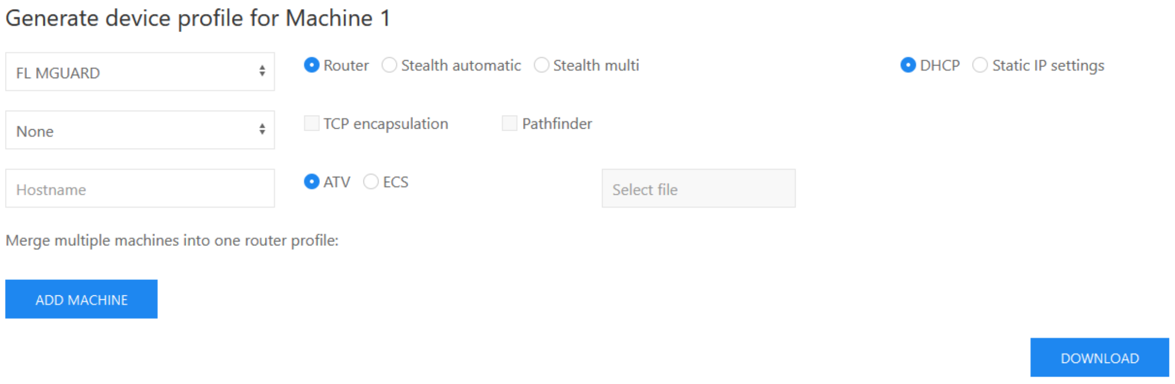
Tag1: All
Tag2: All
Tag3: All

NAME ↓	DAYS LEFT	NAT	NET ↓	ACTIVE
Machine 1	999		7.0.0.1/24	

Figure 21: VPN MACHINE profile

Via the button *VPN* the administrator is able to automatically generate a VPN profile for machine VPN devices. This feature is activated via a separate license. Primarily supported are different *Phoenix Contact* products.

FL *mGuard*



Generate device profile for Machine 1

FL MGUARD

● Router ○ Stealth automatic ○ Stealth multi

● DHCP ○ Static IP settings

None

□ TCP encapsulation □ Pathfinder

Hostname

● ATV ○ ECS

Select file

Merge multiple machines into one router profile:

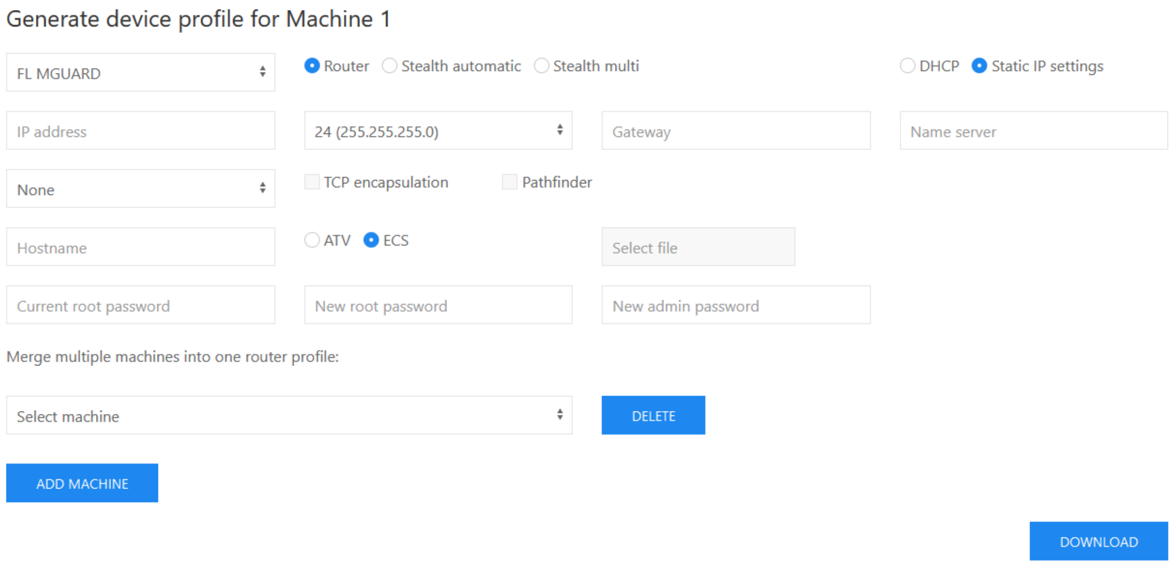
ADD MACHINE

DOWNLOAD

Figure 22: FL mGuard device profile (default window)

- The *mGuard* is able to operate in the mode *Router*, *Stealth automatic* and *Stealth multi*. When selecting the *Router* mode (Figure 22), the *mGuard* acts as a regular router with different LAN and WAN networks. When selecting the *Stealth automatic* mode, the *mGuard* acts as a bridge with only one client connected. When selecting the *Stealth multi* mode, the *mGuard* acts as a bride with a network connected. (Please refer the corresponding *mGuard* manual)
- Selecting the *DHCP* (Dynamic Host Configuration Protocol) option (Figure 22) automatically assigns an IP address to the *mGuard*. Each time the *mGuard* is taken off the network and reconnected the IP address will change. In most scenarios this choice is the preferred selection. Selecting the *Static IP settings* option (Figure 23) will reveal additional options. The administrator needs to assign a static *IP address*, chose a netmask, assign a *Gateway* and a *Name server*.
- (Optional) The VPN tunnel of the *mGuard* can be switched on and off via a hardware contact. If *None* is left unchanged it will not be possible to switch the VPN via the hardware contact. Selecting either the *Switch* or the *Push button* activates the feature. (Figure 22)
- (Optional and licensed) Selecting the *TCP encapsulation* (Transmission Control Protocol) option wraps the individual VPN packets into TCP. This feature is only available if the external *mGuard* is run as a machine gateway which is licensed. Selecting the *Pathfinder* option warps the individual VPN packets into TCP utilizing the *pathfinder* technology. Selecting either of these options will limit the performance of the VPN tunnel. (Figure 22)
- (Optional) Assigning a *Hostname* creates a redundancy that allows the VPN device to be addressed via the web browser's search bar in addition to the IP address. (Figure 22)
- The *ATV* file format (Figure 22) is used to upload the configuration via the *mGuard* web shell. If the *ECS* file format is selected (Figure 23), the configuration is transferred to the *mGuard* via a SD-card. In this case the *MS* requests the root-password. It is possible to assign a new root-password. If the field is left blank, the *mGuard*'s default password will be set. The previous password can be set again if the root-password is not supposed to change.
- (Optional) Additional variables can be uploaded to the VPN device via the *Select file* option. Supported file formats are ATV fragment data. (Figure 22)

- (Optional) Via the *Merge multiple machines into one router profile* option it is possible to place multiple machines behind one *mGuard*. (Figure 23)



Generate device profile for Machine 1

FL MGUARD

● Router ○ Stealth automatic ○ Stealth multi

○ DHCP ● Static IP settings

IP address | 24 (255.255.255.0) | Gateway | Name server

None

□ TCP encapsulation □ Pathfinder

Hostname

○ ATV ● ECS

Select file

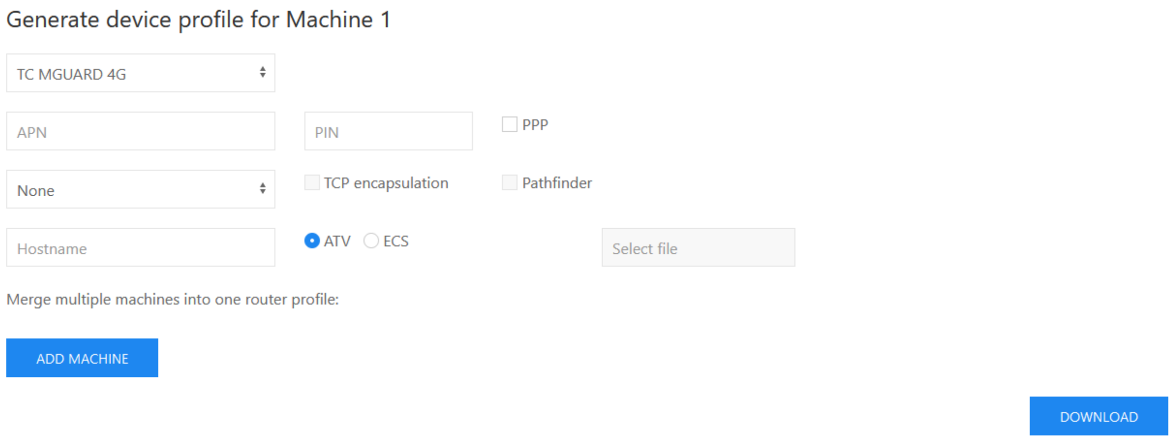
Current root password | New root password | New admin password

Merge multiple machines into one router profile:

Select machine

Figure 23: FL mGuard device profile (Static IP enabled; ECS enabled; Merge multiple machines extended)

TC *mGuard* 4G



Generate device profile for Machine 1

TC MGUARD 4G

APN | PIN | □ PPP

None

□ TCP encapsulation □ Pathfinder

Hostname

● ATV ○ ECS

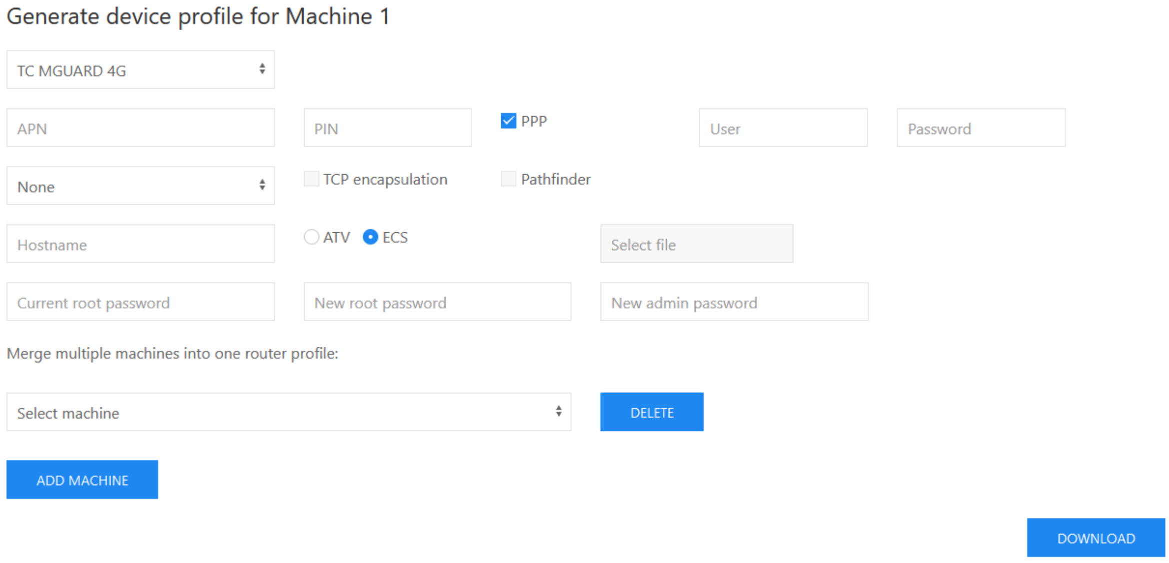
Select file

Merge multiple machines into one router profile:

Figure 24: TC mGuard 4G device profile (default window)

- The APN (Access Point Name) is provided by the mobile provider. (Figure 24)
- The *PIN* textbox needs to be filled with the valid SIM pin. (Figure 24)
- (Optional) The checkbox *PPP* needs to be checked should the mobile provider require a PPP (Point-to-Point Protocol) authentication. The administrator needs to assign a *User* and a *Password* if this box is checked. (Figure 25)
- (Optional) The VPN tunnel of the *mGuard* can be switched on and off via a hardware contact. If *None* is left unchanged it will not be possible to switch the VPN via the hardware contact. Selecting either the *Switch* or the *Push button* activates the feature. (Figure 24)

- (Optional and licensed) Selecting the *TCP encapsulation* (Transmission Control Protocol) option wraps the individual VPN packets into TCP. This feature is only available if the external *mGuard* is run as a machine gateway which is licensed. Selecting the *Pathfinder* option warps the individual VPN packets into TCP utilizing the *pathfinder* technology. Selecting either of these options will limit the performance of the VPN tunnel. (Figure 24)
- (Optional) Assigning a *Hostname* creates a redundancy that allows the VPN device to be addressed via the web browser's search bar in addition to the IP address. (Figure 24)
- The *ATV* file format (Figure 24) is used to upload the configuration via the *mGuard* web shell. If the *ECS* file format is selected (Figure 25), the configuration is transferred to the *mGuard* via a SD-card. In this case the *MS* requests the root-password. It is possible to assign a new root-password. If the field is left blank, the *mGuard*'s default password will be set. The previous password can be set again if the root-password is not supposed to change.
- (Optional) Additional variables can be uploaded to the VPN device via the *Select file* option. Supported file formats are ATV fragment data. (Figure 24)
- (Optional) Via the *Merge multiple machines into one router profile* option it is possible to place multiple machines behind one *mGuard*. (Figure 25)



Generate device profile for Machine 1

TC MGUARD 4G

APN | PIN | ☑ PPP | User | Password

None | □ TCP encapsulation | □ Pathfinder

Hostname | ○ ATV ● ECS | Select file

Current root password | New root password | New admin password

Merge multiple machines into one router profile:

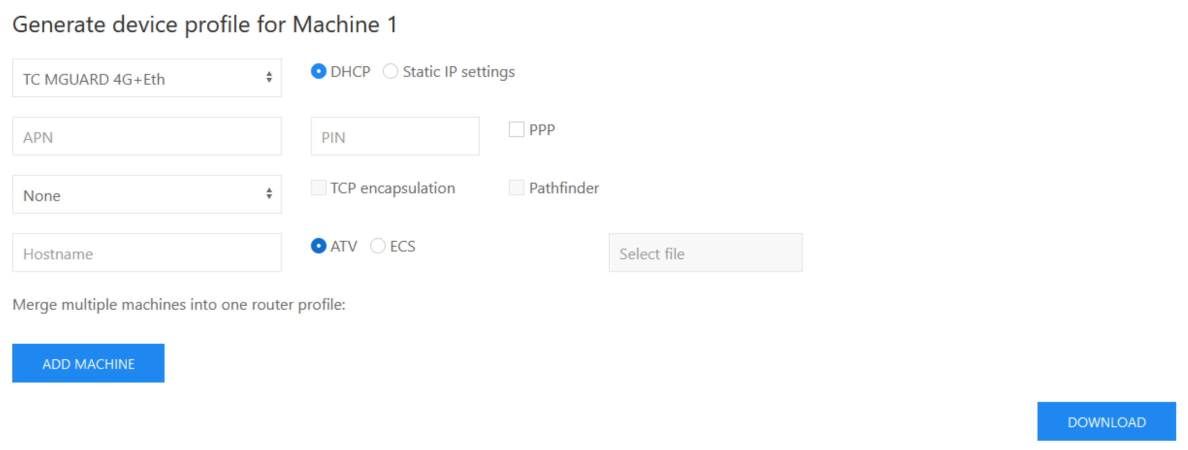
Select machine | DELETE

ADD MACHINE

DOWNLOAD

Figure 25: TC mGuard 4G device profile (PPP enabled; ECS enabled; Merge multiple machines extended)

TC *mGuard* 4G + Eth



Generate device profile for Machine 1

TC MGUARD 4G+Eth

● DHCP ○ Static IP settings

APN

PIN

□ PPP

None

□ TCP encapsulation

□ Pathfinder

Hostname

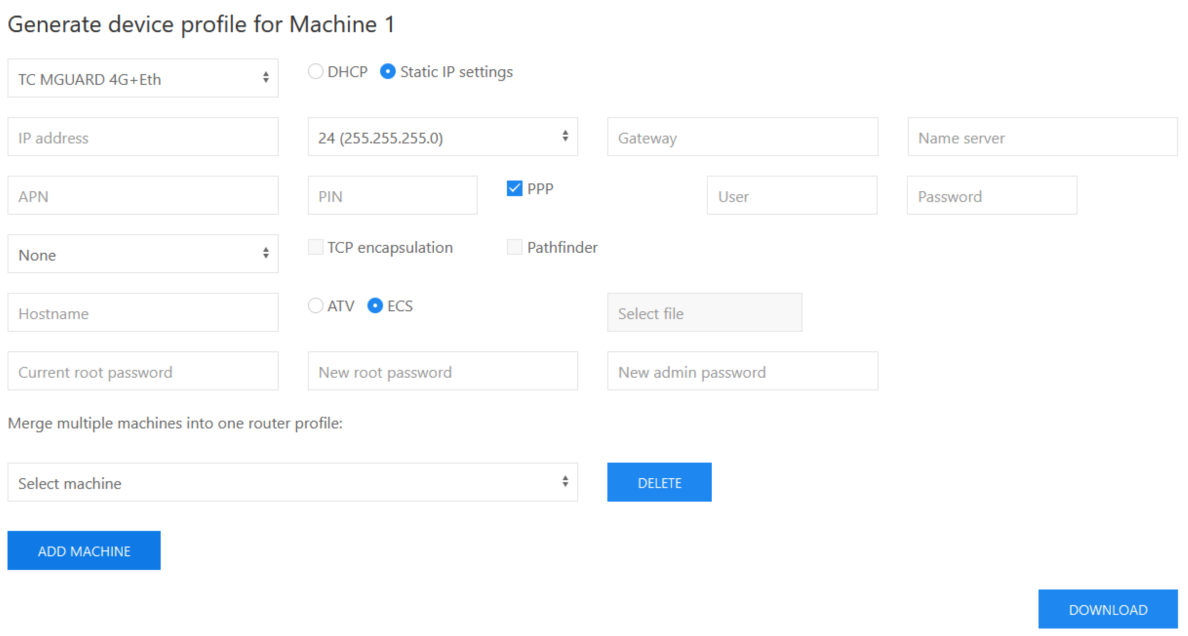
● ATV ○ ECS

Select file

Merge multiple machines into one router profile:

Figure 26: TC mGuard 4G + Eth device profile (default window)

- Selecting the *DHCP* (Dynamic Host Configuration Protocol) option (Figure 26) automatically assigns an IP address to the *mGuard*. Each time the *mGuard* is taken off the network and reconnected the IP address will change. In most scenarios this choice is the preferred selection. Selecting the *Static IP settings* option (Figure 27) will reveal additional options. The administrator needs to assign a static *IP address*, chose a netmask, assign a *Gateway* and a *Name server*.
- The APN (Access Point Name) is provided by the mobile provider. (Figure 26)
- The *PIN* textbox needs to be filled with the valid SIM pin. (Figure 26)
- (Optional) The checkbox *PPP* needs to be checked should the mobile provider require a PPP (Point-to-Point Protocol) authentication. The administrator needs to assign a *User* and a *Password* if this box is checked. (Figure 27)
- (Optional) The VPN tunnel of the *mGuard* can be switched on and off via a hardware contact. If *None* is left unchanged it will not be possible to switch the VPN via the hardware contact. Selecting either the *Switch* or the *Push button* activates the feature. (Figure 26)
- (Optional and licensed) Selecting the *TCP encapsulation* (Transmission Control Protocol) option wraps the individual VPN packets into TCP. This feature is only available if the external *mGuard* is run as a machine gateway which is licensed. Selecting the *Pathfinder* option warps the individual VPN packets into TCP utilizing the *pathfinder* technology. Selecting either of these options will limit the performance of the VPN tunnel. (Figure 26)
- (Optional) Assigning a *Hostname* creates a redundancy that allows the VPN device to be addressed via the web browser’s search bar in addition to the IP address. (Figure 26)
- The *ATV* file format (Figure 26) is used to upload the configuration via the *mGuard* web shell. If the *ECS* file format is selected (Figure 27), the configuration is transferred to the *mGuard* via a SD-card. In this case the *MS* requests the root-password. It is possible to assign a new root-password. If the field is left blank, the *mGuard*’s default password will be set. The previous password can be set again if the root-password is not supposed to change.
- (Optional) Additional variables can be uploaded to the VPN device via the *Select file* option. Supported file formats are ATV fragment data. (Figure 26)
- (Optional) Via the *Merge multiple machines into one router profile* option it is possible to place multiple machines behind one *mGuard*. (Figure 27)



Generate device profile for Machine 1

TC MGUARD 4G+Eth ○ DHCP ● Static IP settings

IP address | 24 (255.255.255.0) | Gateway | Name server

APN | PIN | ☑ PPP | User | Password

None | □ TCP encapsulation | □ Pathfinder

Hostname | ○ ATV ● ECS | Select file

Current root password | New root password | New admin password

Merge multiple machines into one router profile:

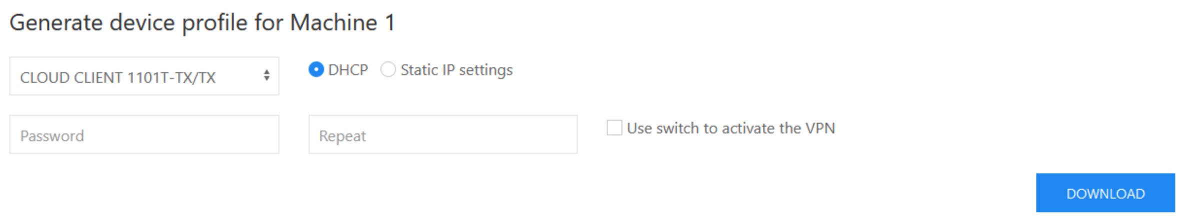
Select machine | DELETE

ADD MACHINE

DOWNLOAD

Figure 27: TC mGuard 4G + Eth device profile (Static IP enabled; PPP enabled; ECS enabled; Merge multiple machines extended)

CLOUD CLIENT 1101T-TX/TX



Generate device profile for Machine 1

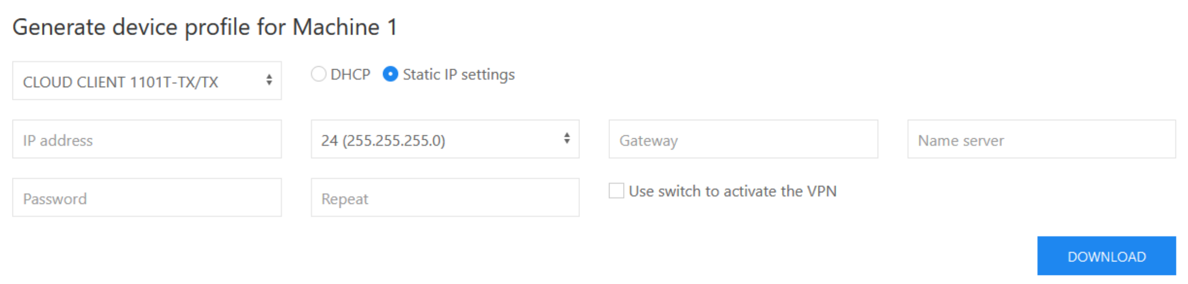
CLOUD CLIENT 1101T-TX/TX ● DHCP ○ Static IP settings

Password | Repeat | □ Use switch to activate the VPN

DOWNLOAD

Figure 28: CLOUD CLIENT 1101T-TX/TX device profile (default window)

- Selecting the *DHCP* (Dynamic Host Configuration Protocol) option (Figure 28) automatically assigns an IP address to the *mGuard*. Each time the *mGuard* is taken off the network and reconnected the IP address will change. In most scenarios this choice is the preferred selection. Selecting the *Static IP settings* option (Figure 29) will reveal additional options. The administrator needs to assign a static *IP address*, chose a netmask, assign a *Gateway* and a *Name server*.
- The textbox *Password* sets up an administrator password for the target device. This password needs to be repeated via the *Repeat* textbox. (Figure 28)
- (Optional) The VPN tunnel of the *CLOUD CLIENT* can be switched on and off via a hardware contact. This feature will be activated by checking the checkbox *Use switch to activate the VPN*. (Figure 28)



Generate device profile for Machine 1

CLOUD CLIENT 1101T-TX/TX

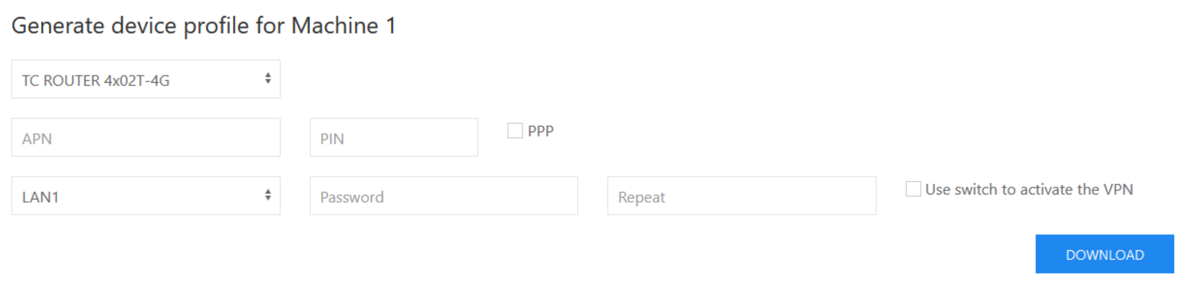
○ DHCP ● Static IP settings

IP address | 24 (255.255.255.0) | Gateway | Name server

Password | Repeat | □ Use switch to activate the VPN

Figure 29: CLOUD CLIENT 1191T-TX/TX device profile (Static IP enabled)

TC ROUTER 4x02T – 4G



Generate device profile for Machine 1

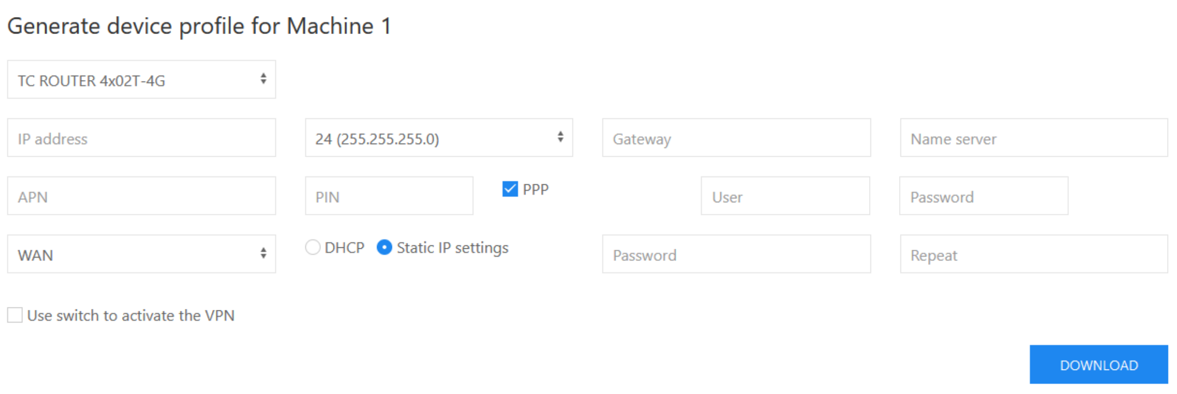
TC ROUTER 4x02T-4G

APN | PIN | □ PPP

LAN1 | Password | Repeat | □ Use switch to activate the VPN

Figure 30: TC ROUTER 4x02T - 4G device profile (default window)

- The APN (Access Point Name) is provided by the mobile provider. (Figure 30)
- The *PIN* textbox needs to be filled with the valid SIM pin. (Figure 30)
- (Optional) The checkbox *PPP* needs to be checked should the mobile provider require a PPP (Point-to-Point Protocol) authentication. The administrator needs to assign a *User* and a *Password* if this box is checked. (Figure 31)
- Selecting the *LAN1*/*WAN* option determents in which physical port the router operates. In *LAN1* mode (Figure 30) the port is assigned to the internal machine network. A password needs to be set by the administrator. When selecting the *WAN* mode (Figure 31), the port is separated from the internal machine network and can be connected to a higher-level network (for example Internet or production network). The administrator selects either the *DHCP* or the *Static IP settings* (Figure 31) option. Selecting the *DHCP* (Dynamic Host Configuration Protocol) option automatically assigns an IP address to the *mGuard*. Each time the *mGuard* is taken off the network and reconnected the IP address will change. In most scenarios this choice is the preferred selection. Selecting the *Static IP settings* option will reveal additional options. The administrator needs to assign a static *IP address*, chose a netmask, assign a *Gateway* and a *Name server*.
- The textbox *Password* sets up an administrator password for the target device. This password needs to be repeated via the *Repeat* textbox. (Figure 30)
- (Optional) The VPN tunnel of the *TC ROUTER* can be switched on and off via a hardware contact. This feature will be activated by checking the checkbox *Use switch to activate the VPN*. (Figure 30)



Generate device profile for Machine 1

TC ROUTER 4x02T-4G

IP address | 24 (255.255.255.0) | Gateway | Name server

APN | PIN | ☑ PPP | User | Password

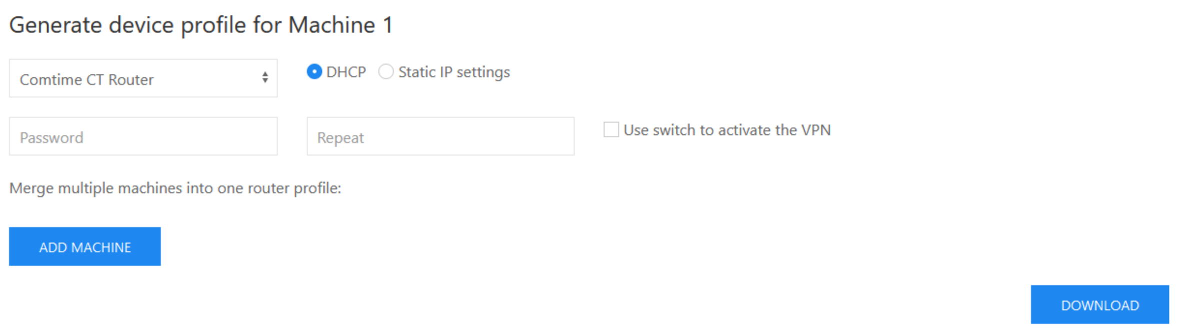
WAN | ○ DHCP ● Static IP settings | Password | Repeat

□ Use switch to activate the VPN

DOWNLOAD

Figure 31: TC ROUTER 4x02T - 4G device profile (PPP enabled; WAN enabled; Static IP enabled)

Comtime CT Router



Generate device profile for Machine 1

Comtime CT Router | ● DHCP ○ Static IP settings

Password | Repeat | □ Use switch to activate the VPN

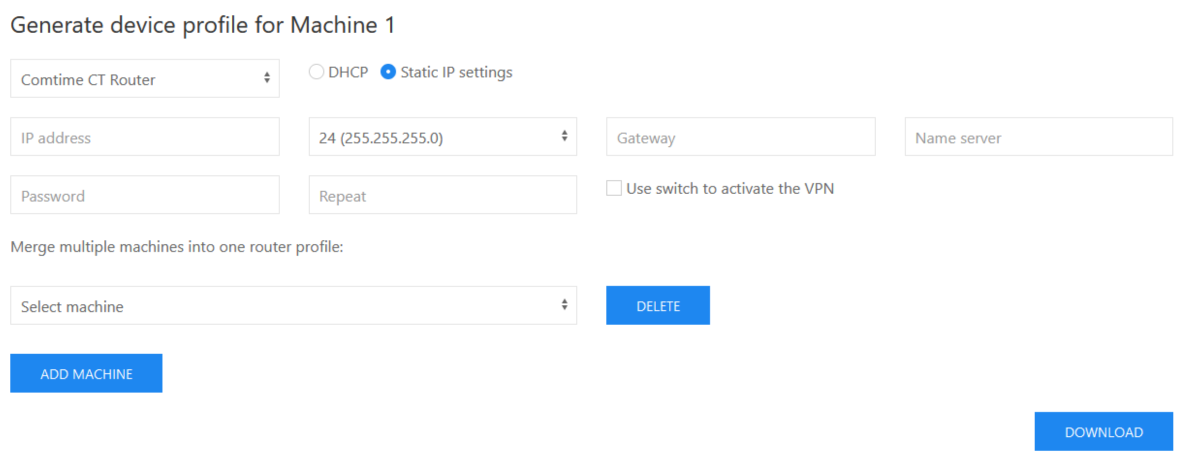
Merge multiple machines into one router profile:

ADD MACHINE

DOWNLOAD

Figure 32: Comtime CT Router device profile (default window)

- Selecting the *DHCP* (Dynamic Host Configuration Protocol) option (Figure 32) automatically assigns an IP address to the *mGuard*. Each time the *mGuard* is taken off the network and reconnected the IP address will change. In most scenarios this choice is the preferred selection. Selecting the *Static IP settings* option (Figure 33) will reveal additional options. The administrator needs to assign a static *IP address*, chose a netmask, assign a *Gateway* and a *Name server*.
- The textbox *Password* sets up an administrator password for the target device. This password needs to be repeated via the *Repeat* textbox. (Figure 32)
- (Optional) The VPN tunnel of the *CT Router* can be switched on and off via a hardware contact. This feature will be activated by checking the checkbox *Use switch to activate the VPN*. (Figure 32)
- (Optional) Via the *Merge multiple machines into one router profile* option it is possible to place multiple machines behind one *mGuard*. (Figure 33)



Generate device profile for Machine 1

Comtime CT Router

○ DHCP ● Static IP settings

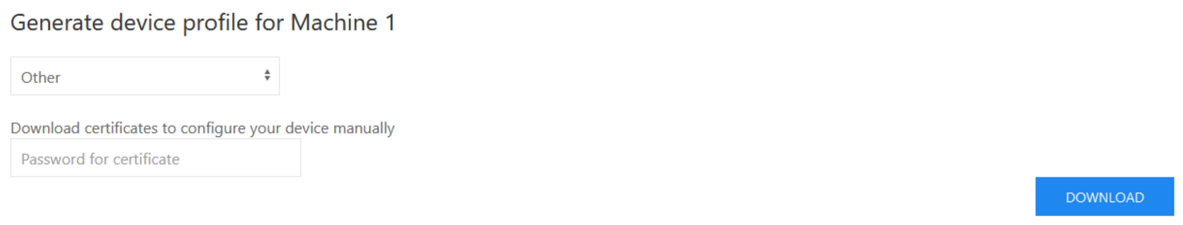
24 (255.255.255.0)

□ Use switch to activate the VPN

Merge multiple machines into one router profile:

Figure 33: Comtime CT Router device profile (Static IP enabled; Merge multiple machines extended)

Other



Generate device profile for Machine 1

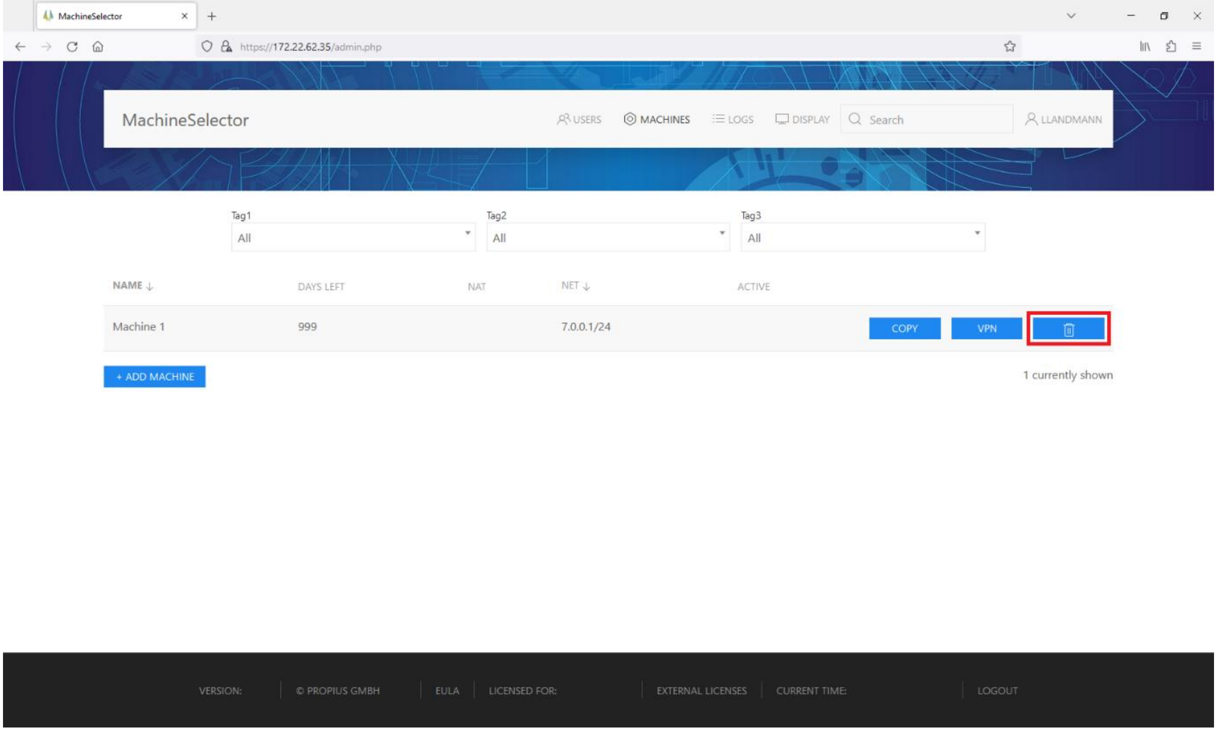
Other

Download certificates to configure your device manually

Figure 34: Other device profile (default window)

- If other devices are being utilized, it is possible to download the corresponding certificates via the MS. The administrator sets the password for the certificate via the *Password for certificate* box. (Figure 34)

8.2.3 Delete Machine



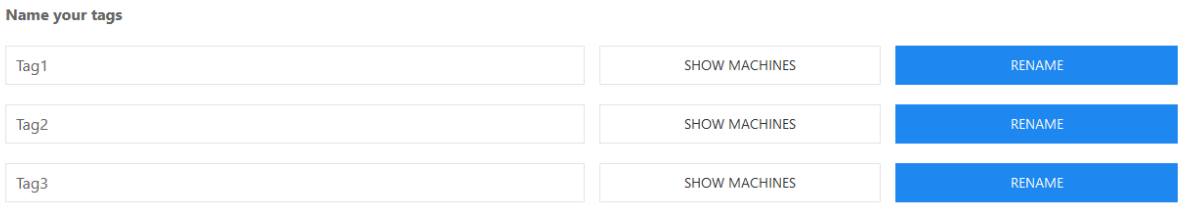
NAME ↓	DAYS LEFT	NAT	NET ↓	ACTIVE			
Machine 1	999		7.0.0.1/24		COPY	VPN	🗑

Figure 35: DELETE MACHINE

In case a machine is no longer needed, it is possible to delete the machine. In order to delete the machine, the administrator selects the trashcan icon next to the desired machine on the *MACHINES* overview page. A deleted machine cannot be recovered.

8.3 Manage tags

In order to edit the tags, the administrator navigates to the *Manage tags* tab by hovering above the *MACHINES* button. (Figure 16)


Name your tags

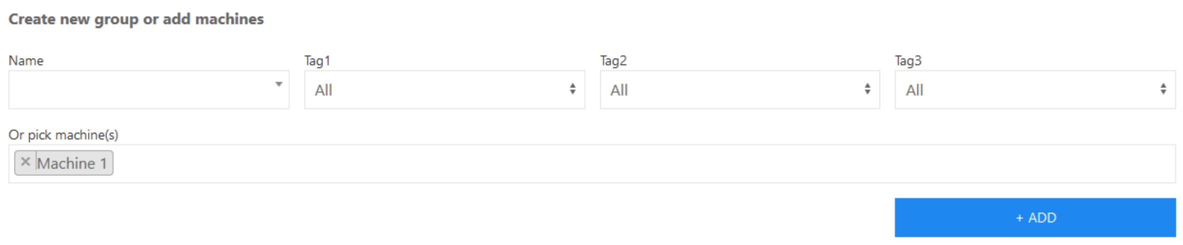
Tag1	SHOW MACHINES	RENAME
Tag2	SHOW MACHINES	RENAME
Tag3	SHOW MACHINES	RENAME

Figure 36: Manage tags window

To rename a default tag, the administrator assigns a new name and confirms the entry via the *RENAME* button. Within this menu it is also possible to filter for machines with certain tags.

8.4 Add permission group

In order to create a new permission group or to add a machine to an existing permission group, the administrator navigates to the *Add permission group* tab by hovering above the *MACHINES* button. (Figure 16)



Create new group or add machines

Name

Tag1: All

Tag2: All

Tag3: All

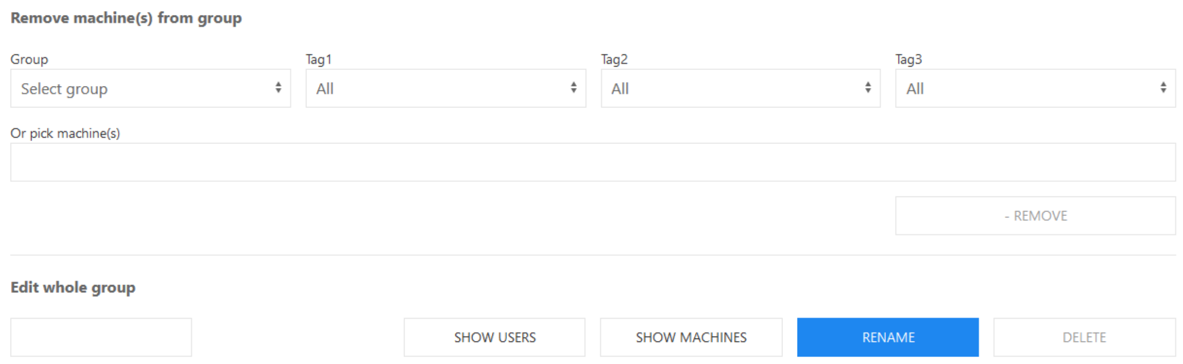
Or pick machine(s): × Machine 1

Figure 37: Add permission group window

After assigning a *Name* and *Tags* or singular machine names, the permission group can be created. Selecting *Tags* adds every machine to the permission group that utilizes this specific tag. Selecting specific machines using the *pick machine(s)* option adds a single machine.

8.5 Edit permission groups

In order to rename or delete a permission group or remove singular machines from a permission group, the administrator navigates to the *Edit permission groups* tab by hovering above the *MACHINES* button. (Figure 16)



Remove machine(s) from group

Group: Select group

Tag1: All

Tag2: All

Tag3: All

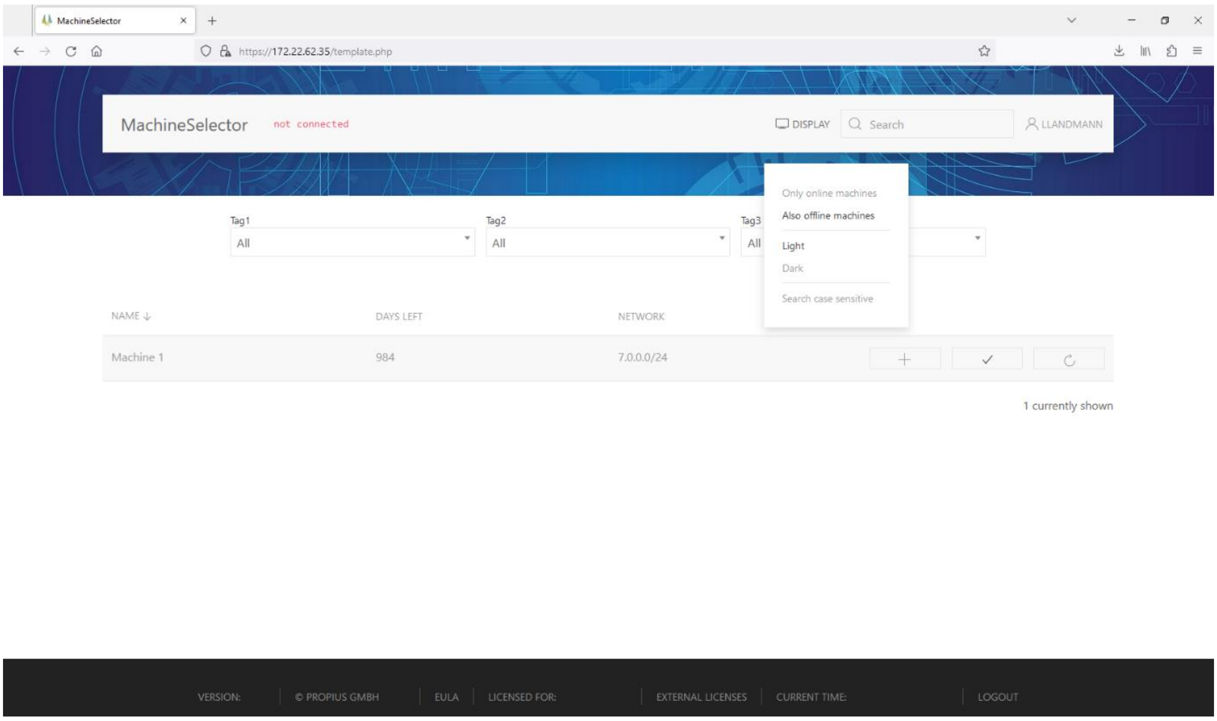
Or pick machine(s)

Edit whole group

Figure 38: Edit permission groups window

- Removing machines from a permission group is achieved by selecting the desired group, selecting a tag (removes all machines utilizing the selected tag) or selecting single machines via the *pick machine(s)* option. Machines selected this way will be deleted from the permission group and cannot be accessed by users assigned to this permission group.
- To delete or rename the whole group, the administrator choses the corresponding buttons. It is also possible to show all users and machines assigned to this permission group via the *SHOW USERS* and *SHOW MACHINES* button.

9 User



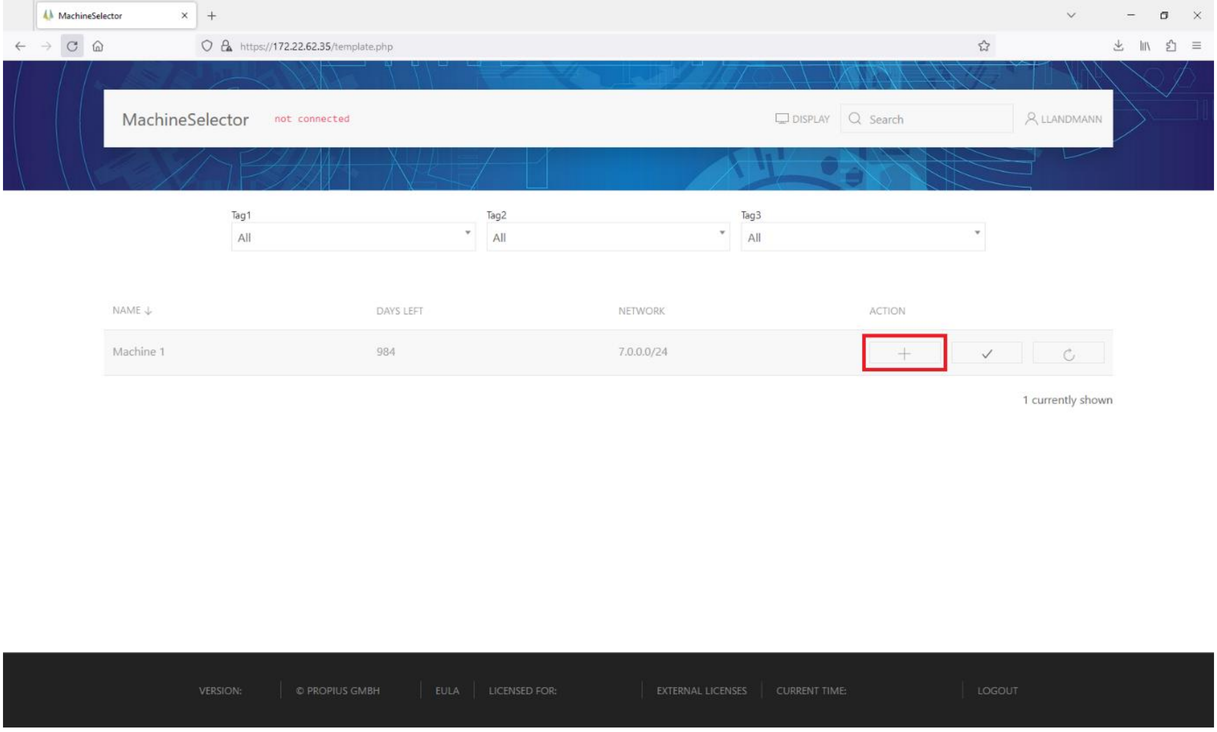
Tag1: All
Tag2: All
Tag3: All

NAME ↓	DAYS LEFT	NETWORK
Machine 1	984	7.0.0.0/24

1 currently shown

Figure 39: User (overview)

9.1 Start routing to a machine



Tag1: All
Tag2: All
Tag3: All

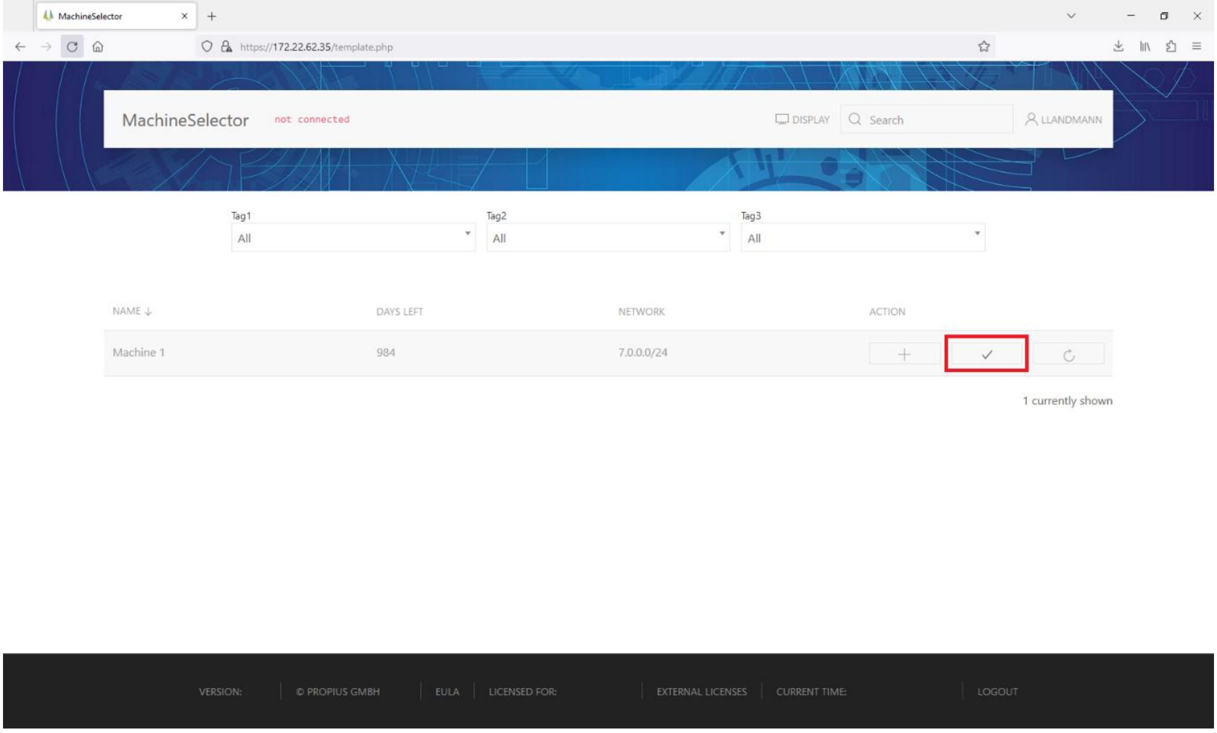
NAME ↓	DAYS LEFT	NETWORK	ACTION
Machine 1	984	7.0.0.0/24	+ ✓

1 currently shown

Figure 40: Start routing to machine

The + button starts the routing to a specific machine from the user's perspective. If the corresponding machine has an active network connection and the user's service connection is established (*OVPN* client or local secure network) the button will appear in blue.

9.2 Check for concurrent connections



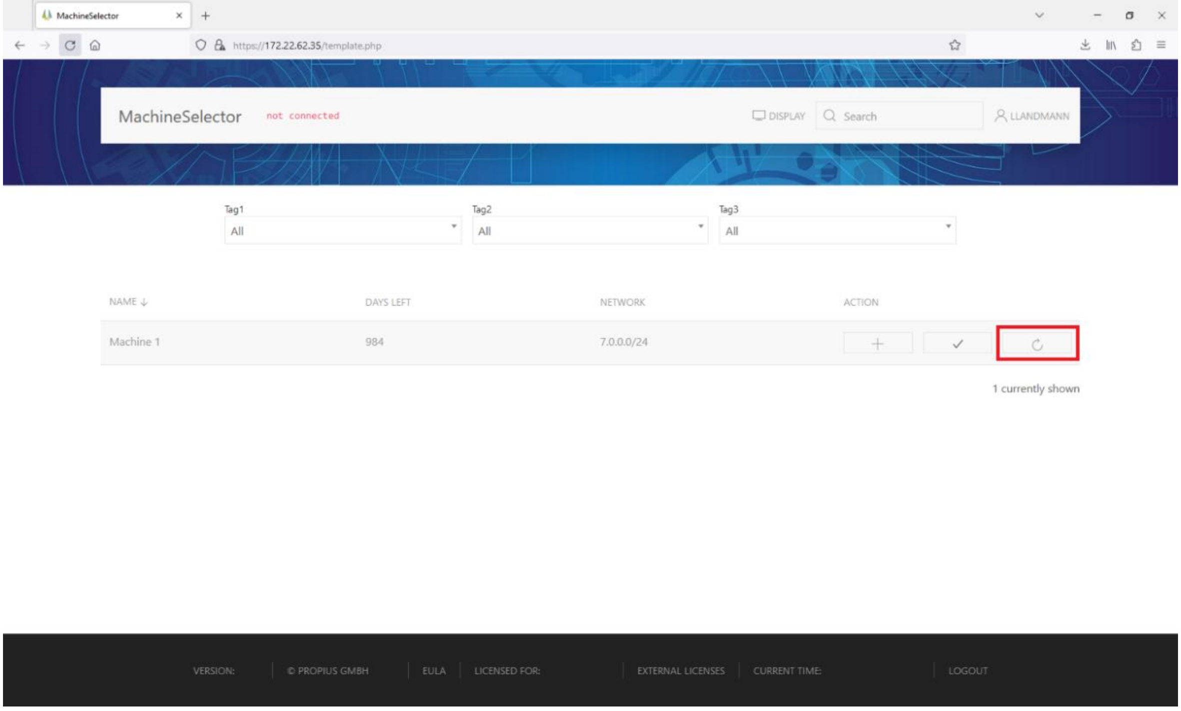
NAME ↓	DAYS LEFT	NETWORK	ACTION
Machine 1	984	7.0.0.0/24	+ ✓ ↻

1 currently shown

Figure 41: Check for concurrent connections

The checkmark button allows the users to check for concurrent connections before establishing a connection themselves. This feature assures that only one user is connected at the same time. Users who connect to a machine that is already connected to will terminate the other user's connection in order to establish their own.

9.3 Restart the *IPsec* machine connection (only if external machine gateway is used)



MachineSelector

https://172.22.62.35/template.php

MachineSelector not connected

Tag1: All

Tag2: All

Tag3: All

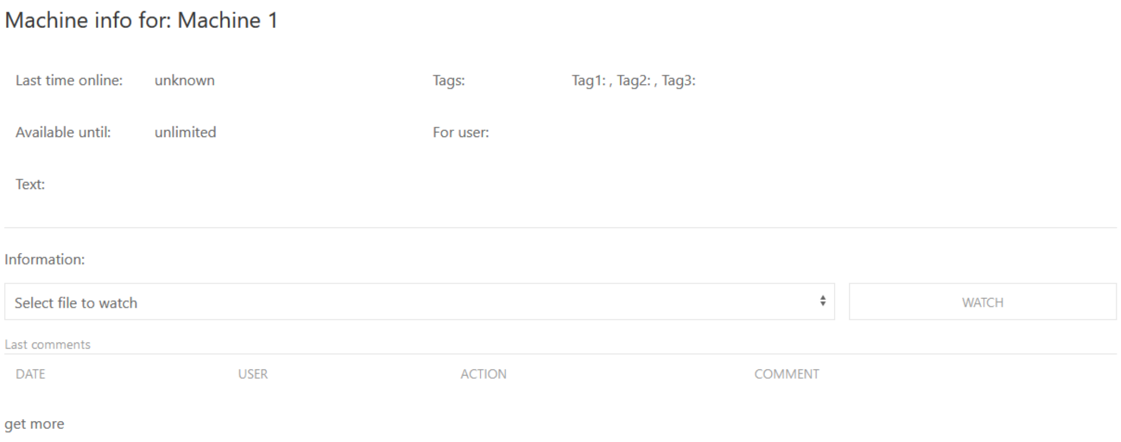
NAME ↓	DAYS LEFT	NETWORK	ACTION
Machine 1	984	7.0.0.0/24	+ ✓ ↻

1 currently shown

Figure 42: Restart the IPsec machine connection

The refresh button allows the user to restart the *IPsec* machine connection. This becomes necessary if said connection is frozen. This feature becomes available if an external service gateway is being utilized.

9.4 Machine information



Machine info for: Machine 1

Last time online: unknown

Tags: Tag1: , Tag2: , Tag3:

Available until: unlimited

For user:

Text:

Information:

Select file to watch

Last comments

DATE	USER	ACTION	COMMENT

get more

Figure 43: Machine information

The user is able to view the machine’s information by selecting the corresponding machine name on the overview page. The machine information displays the last time online, the tags, the availability and the permitted users. Additionally displayed will be the optional text that the administrator assigned and the files that have been uploaded to the machine. The information also displays the last connection to the machine including all additional information. Selecting the *get more* option allows the user to view the last 10 connections.

10 Controller (licensed)

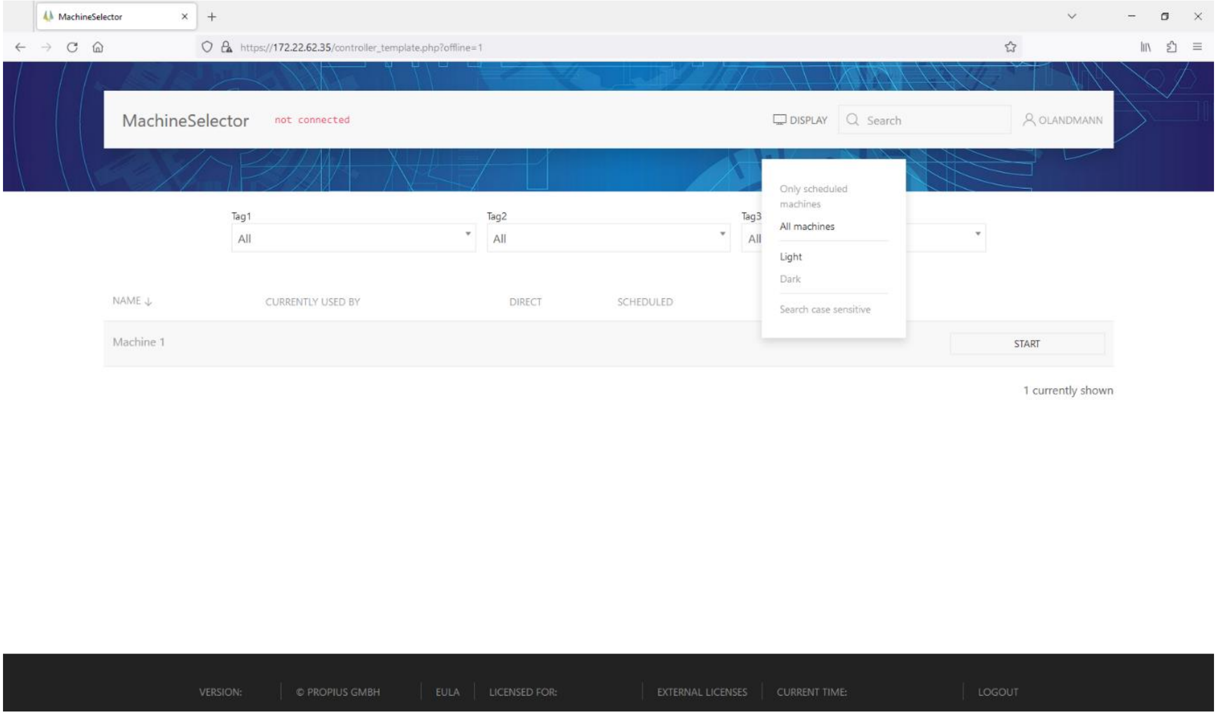


Figure 44: Controller (overview)

10.1 Mode of operation

With the role of the controller, it is possible to schedule a machine for the user to access. Internally this is realized by showing and hiding the machines. Only machines that are set to inactive (see 8.1) can be scheduled by the controller. Machines that are active will be visible to all users with the corresponding permission group.

10.2 Scheduling machines

10.2.1 Filter by machines

By default, the controller will be shown the scheduled machines. These can be filtered for the tags.

The controller is able to filter for nonscheduled machines by hovering above the *DISPLAY* button and selecting *All machines*. (Figure 44) All machines that are created by the administrator(s) will be shown on this tab.

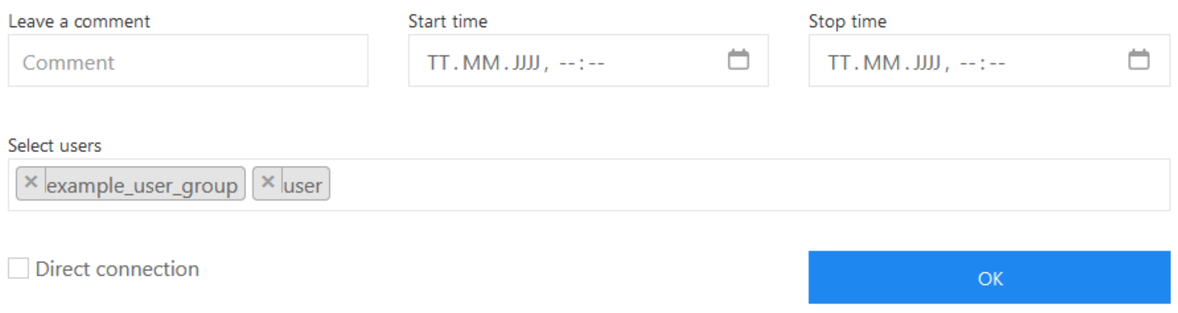
By hovering above the *DISPLAY* button and selecting *Only scheduled machines* it is possible to filter for the current scheduled machines.

10.2.2 Requirement

In order to schedule a machine, the administrator needs to create a machine that is set to inactive by removing the checkmark from the *Active* checkbox (see 8.1).

10.2.3 Execution

Suitable machines can be scheduled by clicking the corresponding *START* button on the *All machines* overview tab. (Figure 44)



Leave a comment

Comment

Start time

TT.MM.JJJJ, --:--

Stop time

TT.MM.JJJJ, --:--

Select users

× example_user_group × user

□ Direct connection

Figure 45: Machine scheduling window

- (Optional) The controller is able to leave a comment when scheduling a machine. This may include the reason for the schedule or a reference person. The comment will be visible to all suitable users and the administrator(s). (Figure 45)
- The controller needs to select a start and a stop time by clicking into the corresponding field. The time will be requested after selecting the date. By default, the maximum time frame is 72 hours (3 days). This value can be edited in the database by *Propius*. (Figure 45)
- By default, the machine will be scheduled for no user. All users can be selected the *All* option. If desired, singular users and user groups (see 5.3) can be selected and deselected by clicking on the corresponding name or clicking the X on the left side of the name. (Figure 45)
- (Optional) The *Direct connection* option allows the user to connect to the machine by only starting the *OVPN* client. Only machines that the user would normally have access to can be accessed. This feature requires *Propius* to activate the user-authentication on the *OVPN* client. (Figure 45)

11 ACCOUNT

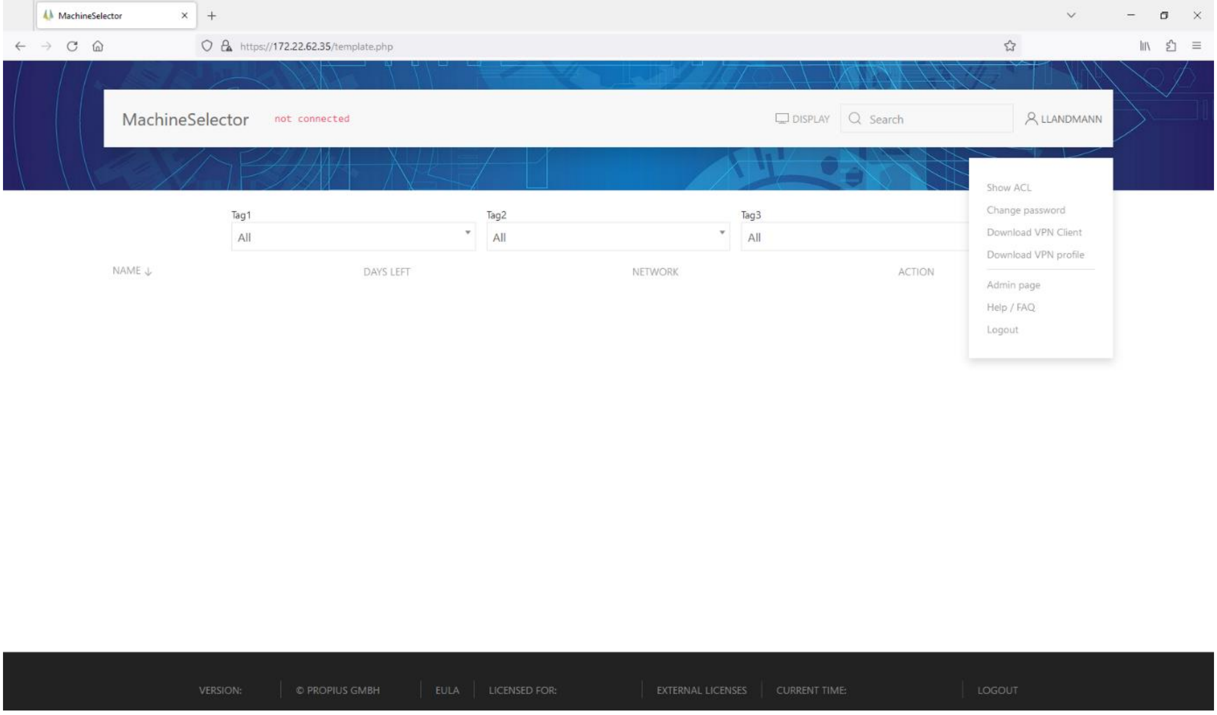
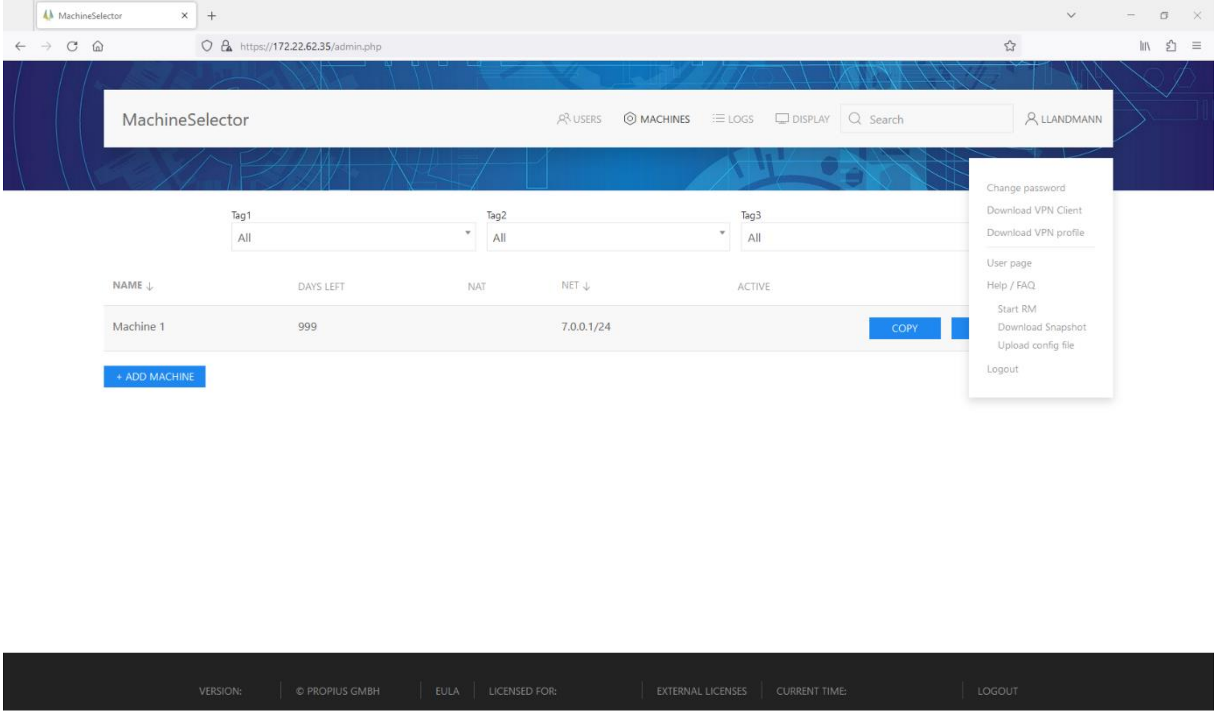


Figure 46: ACCOUNT (overview; user-view)



NAME ↓	DAYS LEFT	NAT	NET ↓	ACTIVE
Machine 1	999		7.0.0.1/24	

Figure 47: ACCOUNT (overview; administrator-view)

11.1 Show ACL (User)

Hovering above the user specific name (user profile) in the top right corner (Figure 46) of the *MachineSelector* (MS) reveals the *Show ACL* option. This grands the users insight on which access control lists (ALC) are assigned to them.

11.2 Change password

Hovering above the user-specific name (user profile) in the top right corner (Figure 46 and Figure 47) of the *MS* reveals the *Change password* option. Any user who does not utilize the LDAP-feature is able to change their password. The password change requires the old password. A new password must contain at least eight characters, one capitalized letter and one number.

11.3 Download VPN Client

Hovering above the user-specific name (user profile) in the top right corner (Figure 46 and Figure 47) of the *MS* reveals the *Download VPN Client* option. This option links the user to the download section of the *OpenVPN* website.

11.4 Download VPN profile

Hovering above the user-specific name (user profile) in the top right corner (Figure 46 and Figure 47) of the *MS* reveals the *Download VPN profile* option. This option downloads the user specific *OpenVPN* profile that can be imported by the *OpenVPN* client.

11.5 Help / FAQ

Hovering above the user-specific name (user profile) in the top right corner (Figure 46 and Figure 47) of the *MS* reveals the *Help / FAQ* section. This option links the user to the *MachineSelector FAQ* section of the *Propius* website.

11.6 Start RM (Administrator)

Hovering above the user-specific name (user profile) in the top right corner (Figure 47) of the *MS* reveals the *Start RM* option. This option establishes a maintenance tunnel to *Propius* (portal1.remoteservice24.com:22002). If the tunnel is no longer needed, navigating to the same location reveals the *Stop RM* option. This disables the tunnel.

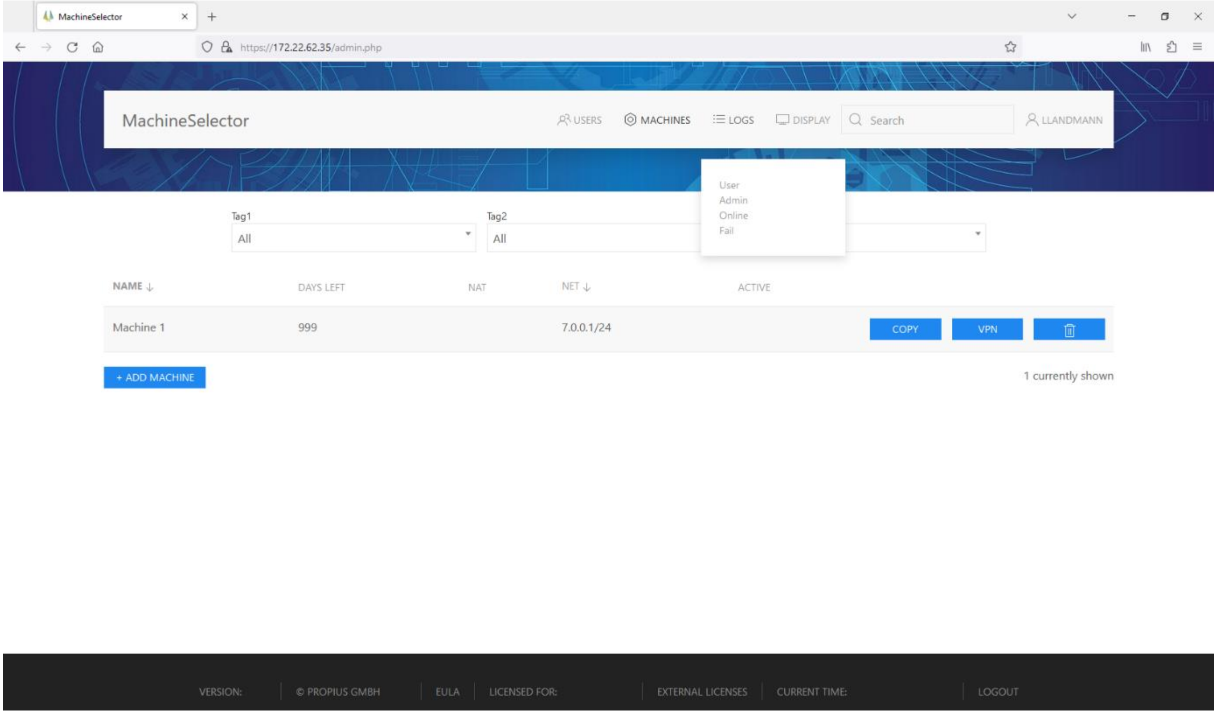
11.7 Download Snapshot (Administrator)

Hovering above the user-specific name (user profile) in the top right corner (Figure 47) of the *MS* reveals the *Download Snapshot* option. This option creates and downloads an encrypted archive. This file allows *Propius* to analyze and rule out issues concerning the *MS* while it is offline. Please attach the file to any support request.

11.8 Upload config file (Administrator)

Hovering above the user-specific name (user profile) in the top right corner Figure 47) of the *MS* reveals the *Upload config file* option. This option allows the user to either configurate the *MS* using a preexisting configuration file or to upgrade the *MS* after purchasing a specific update and/or license.

12 LOGS



NAME ↓	DAYS LEFT	NAT	NET ↓	ACTIVE
Machine 1	999		7.0.0.1/24	

Figure 48: LOGS (overview)

12.1 User

By hovering above the *LOGS* button on the *USERS* or *MACHINES* overview tab (Figure 48) it is possible for the administrator to monitor the actions of all users. This includes login and logout, password changes, started and stopped connections to machines and schedules. Displayed will be the date, time, address, group, username, action, machine and optional comment.

All logs are rotating. They will be sorted by date and time and is possible to arrange the logs in an ascending and descending manner. The logs will be sorted in an ascending manner by default. Via the *Download CSV* button, the logs will be packed and exported as a *.csv* file. This file type is for example used by *Microsoft Excel* and can be imported. Additionally, *Syslog* is also supported. This requires a *Syslog*-server to be entered into the database by *Propius*.

12.2 Admin

By hovering above the *LOGS* button on the *USERS* or *MACHINES* overview tab (Figure 48) it is possible for the administrator to monitor the actions of all administrators. This includes changes to machines, added or deleted users, editing permission groups, access control lists and tags, downloading user profiles and snapshots and starting and stopping a remote access. Displayed will be the date, time, address, group, username, action and the corresponding name.

All logs are rotating. They will be sorted by date and time and is possible to arrange the logs in an ascending and descending manner. The logs will be sorted in an ascending manner by default. Via the *Download CSV* button, the logs will be packed and exported as a *.csv* file. This file type is for example used by *Microsoft Excel* and can be imported. Additionally, *Syslog* is also supported. This requires a *Syslog*-server to be entered into the database by *Propius*.

12.3 Online

By hovering above the *LOGS* button on the *USERS* or *MACHINES* overview tab (Figure 48) it is possible for the administrator to monitor the uptime of all established tunnels. Displayed will be the start date and time, the stop date and time, group, username, machine name and the resulting duration.

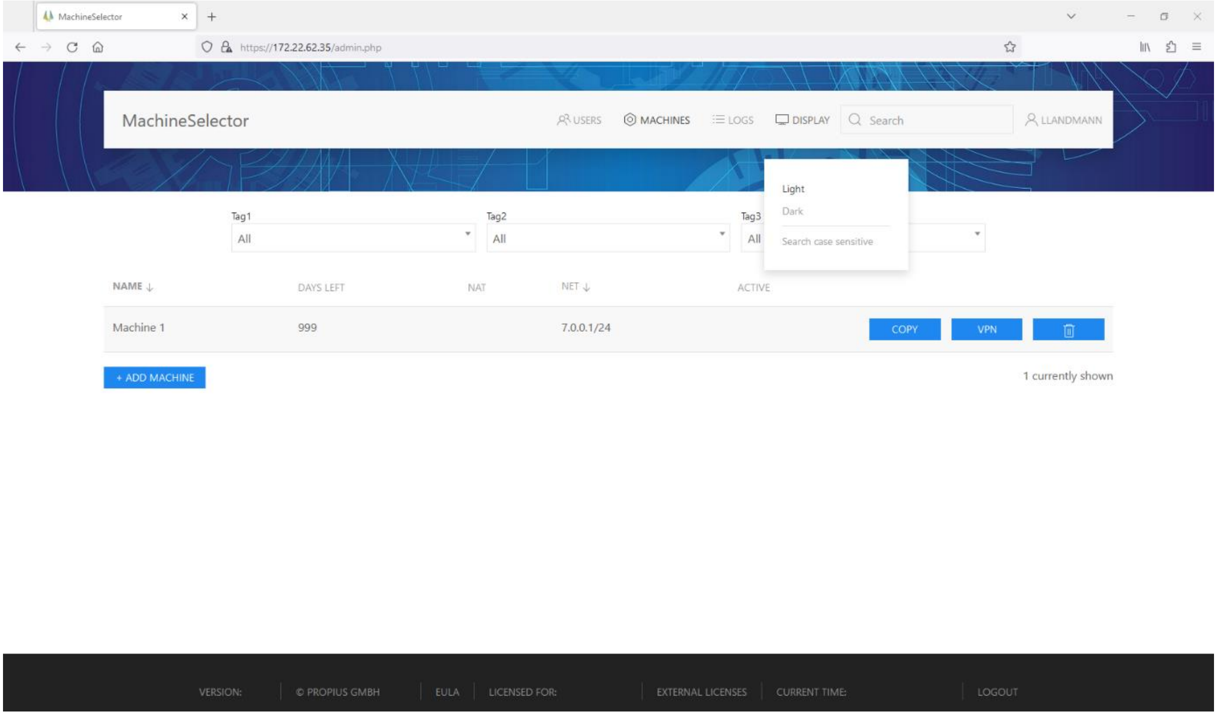
All logs are rotating. They will be sorted by date and time and is possible to arrange the logs in an ascending and descending manner. The logs will be sorted in an ascending manner by default. Via the *Download CSV* button, the logs will be packed and exported as a *.csv* file. This file type is for example used by *Microsoft Excel* and can be imported. Additionally, *Syslog* is also supported. This requires a *Syslog*-server to be entered into the database by *Propius*.

12.4 Fail

By hovering above the *LOGS* button on the *USERS* or *MACHINES* overview tab (Figure 48) it is possible for the administrator to monitor the failed login attempts. Displayed will be the date and time, IP address, group, username and the error message.

All logs are rotating. They will be sorted by date and time and is possible to arrange the logs in an ascending and descending manner. The logs will be sorted in an ascending manner by default. Via the *Download CSV* button, the logs will be packed and exported as a *.csv* file. This file type is for example used by *Microsoft Excel* and can be imported. Additionally, *Syslog* is also supported. This requires a *Syslog*-server to be entered into the database by *Propius*.

13 DISPLAY



NAME ↓	DAYS LEFT	NAT	NET ↓	ACTIVE
Machine 1	999		7.0.0.1/24	

Figure 49: DISPLAY (overview)

13.1 Light/Dark Mode

It is possible to switch between the light and dark mode by hovering above the *DISPLAY* button on the *USERS* or *MACHINES* overview tab. (Figure 49) By default the settings of the operating system will be adopted.

13.2 Search case sensitive

By default, the search bar disregards capital letters. This allows for a broader range of results when searching for users and machines. If desired, it is possible to enable the case sensitive search by hovering above the *DISPLAY* button on the *USERS* or *MACHINES* overview tab. (Figure 49) In order to disable the case sensitive search, the user navigates to the same location and selects *Search case sensitive* again.

14 FAQ

Please refer our FAQ web page: https://www.propius.de/ms-help.html