ENSTO E-RTU 2020 cabinet

System Configuration

4PR-F8-H

Ensto Novexia SAS 210 rue Léon Jouhaux
BP 10446
69656 Villefranche-sur-Saône Cedex,
France

Tel. +33 (0)4 74 65 61 61
Fax +33 (0)4 74 62 96 57

Content

1 "SYSTEM" TAB 4
1.1 TIME AND DATE CONFIGURATION 4
1.2 SOFTWARE UPDATE 5
1.3 CONFIGURATION FILE 5
1.4 REBOOT 6
1.5 RESTORE 6
1.6 SESSION PARAMETERS 7
2 "PASSWORD" TAB 8
3 "USERS" TAB 9
4 "ADD USER" TAB 10
5 "FIREWALL" TAB 11
5.1. FIREWALL STATUS 11
5.2. DoS (DENIAL OF SERVICE) PROTECTION CONFIGURATION 12
5.3. FIREWALL RULES CONFIGURATION 13
5.4. PING CONFIGURATION 14
6 "NTP" TAB 14
6.1. NTP CLIENT STATUS 15
6.2. NTP CLIENT CONFIGURATION 15
7 "OpenVPN" tab 16
7.1. OPENVPN SERVER STATUS 16
7.2. OPENVPN SERVER CONFIGURATION 16
8 "IPSec" tab 18
8.1 IPSEC TUNNEL STATUS 18
8.2 IPSEC TUNNEL CONFIGURATION 18
9 "DHCP" tab 21
9.1. DHCP SERVER STATUS 21
9.2. DHCP SERVER CONFIGURATION 21
9.3. IP ADDRESSES ALLOCATED 22
10 "SSH" tab 23
10.1. SSH SERVER STATUS 23
10.2. SSH SERVER CONFIGURATION 23
11 "WEB server" tab 24

11.1. WEB SERVER STATUS 24
11.2. WEB SERVER CONFIGURATION 24
12 “Encryption Keys and Certificates” tab 26
12.1. CRL 26
12.2. WEB SERVER 27
12.3. OPENVPN 29
12.4. IPSec 30

1 "SYSTEM" TAB

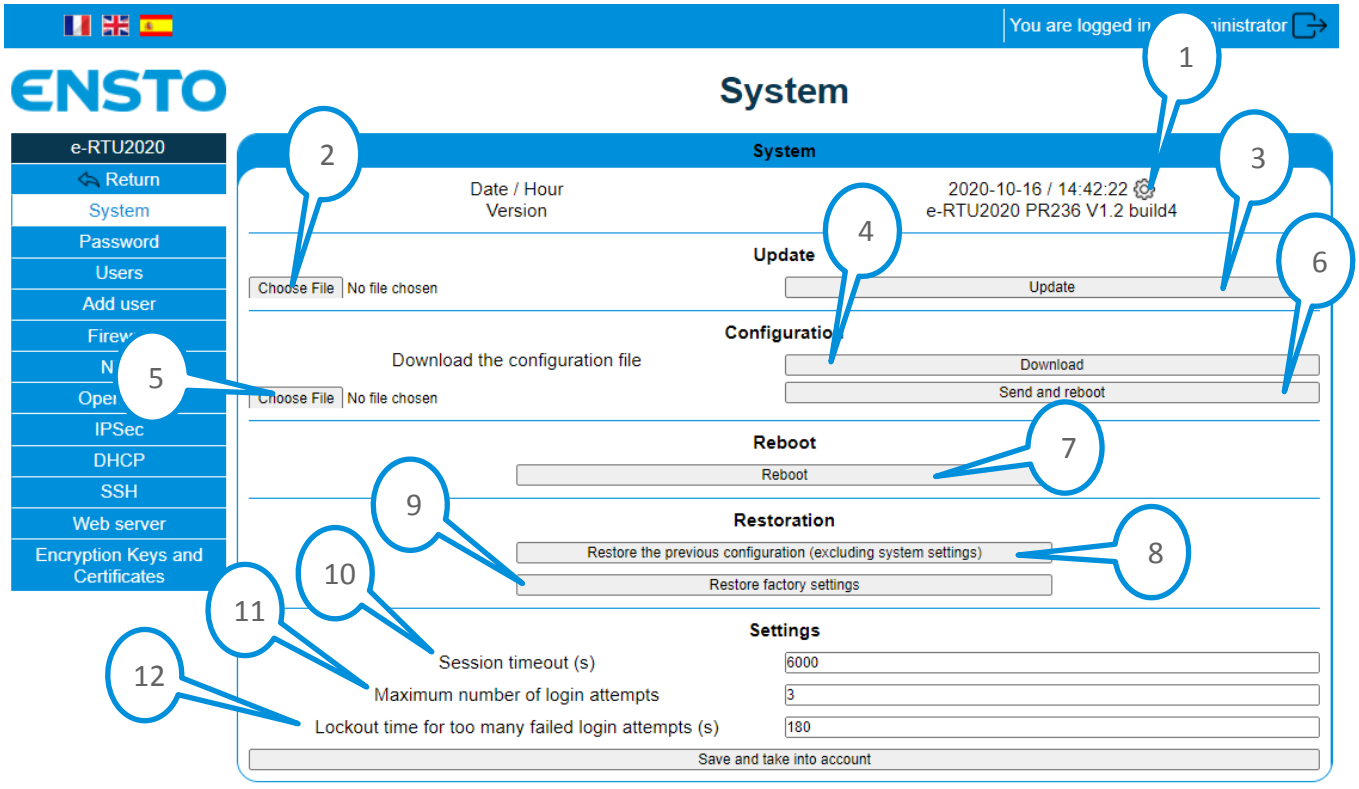

Figure 1: "System" tab

1.1 TIME AND DATE CONFIGURATION

To configure the cabinet's time and date, go to the "System" page "System" tab (Figure 1):

- Click on the cogwheel (1) to open the following dialog box:

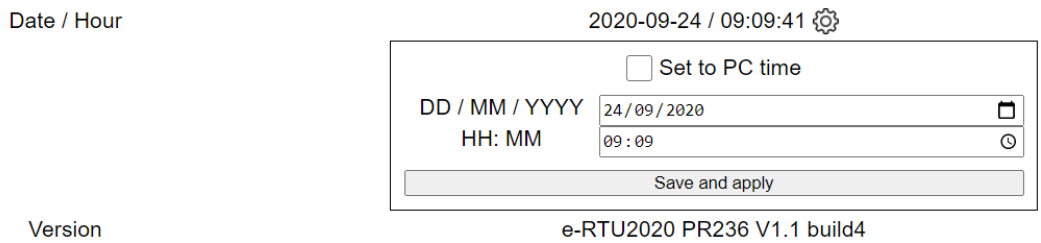

Figure 2: Time and date configuration dialog box

To set the cabinet to the time and date of your PC, in the dialog box (Figure 2):

- Click on the "Set to PC time" box
- Click on "Save and apply"

To update the time and date manually, in the dialog box (Figure 2):

- Complete the “DD / MM / YYYY” and “HH : MM” fields as required
- Click on “Save and apply”

Note: You may be disconnected when applying the time change.

1.2 SOFTWARE UPDATE

To update the cabinet’s software, go to the “System” page “System” tab (Figure 1):

- Click on “Select a file” (2) in the “Update” section
- Depending on your internet browser, a dialog box opens
- Select the corresponding software ZIP file
- Click on “Update” (3)
- Wait for the transfer to finish
- The following dialog box opens:

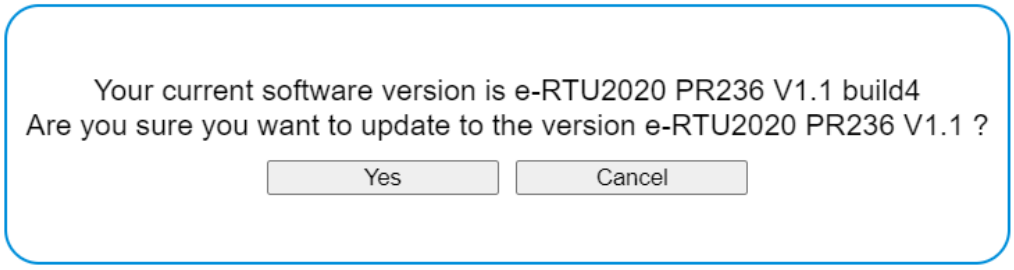

Figure 3: Software update dialog box

- Click on “Yes” to confirm the update or “Cancel” to cancel it
- Wait for the update to finish

Note: The update is complete when the web server connection page appears
Note: It is not possible to return to a previous version of the software

1.3 CONFIGURATION FILE

To download the cabinet’s configuration file, go to the “System” page “System” tab (Figure 1):

- Click on “Download” (4) in the “Configuration” section
- Depending on your internet browser, the configuration ZIP file is downloaded

To send the configuration file to the cabinet, go to the “System” page “System” tab (Figure 1):

- Click on “Select a file” (5) in the “Configuration” section
- Depending on your internet browser, a dialog box opens
- Select the corresponding configuration ZIP file
- Click on “Send and reboot” (6)
- The following dialog box opens:

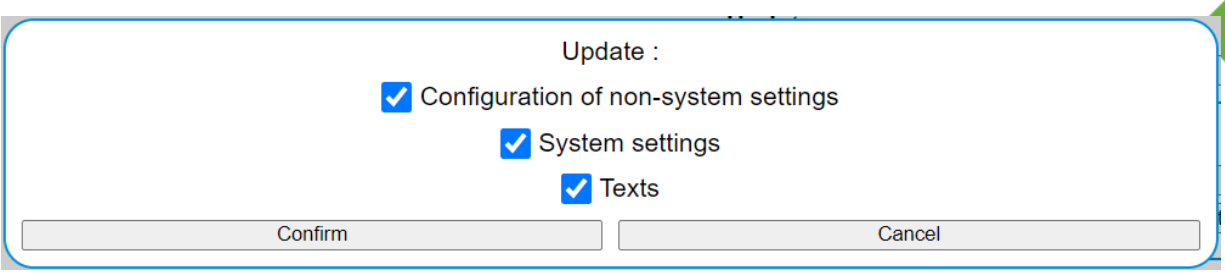

Figure 4: Dialog box for sending the configuration file

- Depending on what you want to configure, select:
  - "Configuration of non-system settings" to configure all the settings, apart from those that are on the "System" page, from the file, example: communication settings, automation settings, etc.
  - "System settings" to configure all the settings that are on the "System" page, from the file, example: VPN settings, Firewall, etc.
  - "Text" to configure all the display text
- Click on "Confirm" to apply the configuration or on "Cancel" to cancel
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears

1.4 REBOOT

To reboot the cabinet, go to the "System" page "System" tab (Figure 1):

- Click on "Reboot" (7) in the "Reboot" section
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears

1.5 RESTORE

When changes to settings (excluding settings on the "System" page) have been made, but you have not clicked on "Apply changes", it is possible to go back and cancel the changes.
It is also possible to restore the cabinet's factory settings.

To cancel current changes, go to the "System" page "System" tab (Figure 1):

- Click on "Restore the previous configuration (excluding system settings)" (8) in the "Restore" section
- The following dialog box opens:

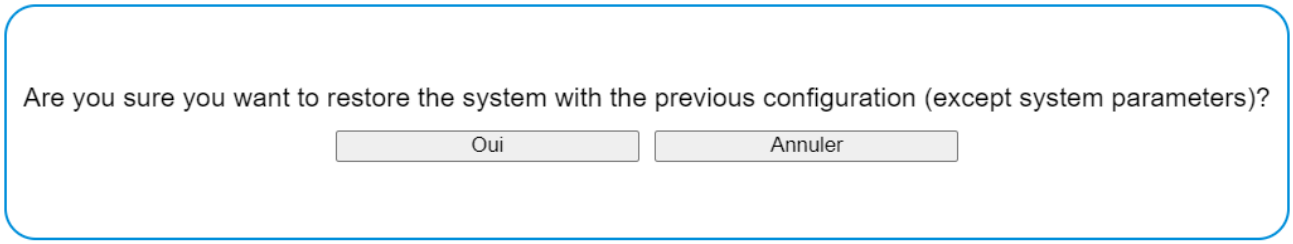

Figure 5: Dialog box for cancelling changes to settings

- Click on “Yes” to confirm the cancellation of changes to settings or on “Cancel” to cancel
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears

To restore the cabinet’s factory settings **(for users with “Administrator” rights only)**, go to the “System” page “System” tab (Figure 1):

- Click on “Restore factory settings” (9) in the “Restore” section
- The following dialog box opens:

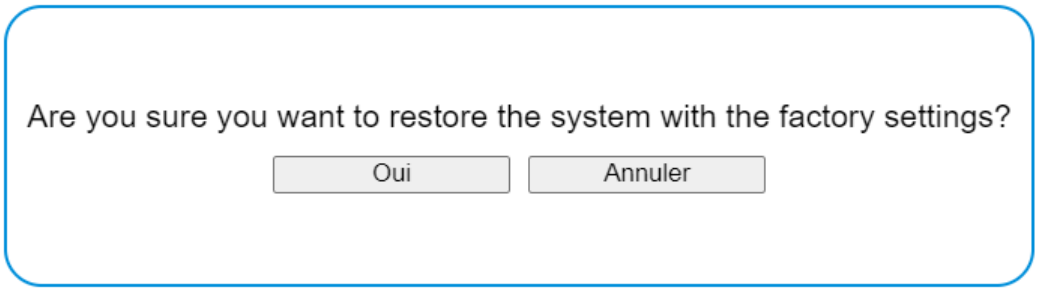

Figure 6: Dialog box for restoring factory settings

- Click on “Yes” to confirm the restoration of factory settings or on “Cancel” to cancel
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears

1.6 SESSION PARAMETERS

To configure the session parameters for web pages **(for users with “Administrator” rights only)**, go to the “System” page “System” tab (Figure 1):

- Complete the “Session timeout(s)” field (10) to define the log out time in seconds when the user does not perform any actions on web pages
- Complete the “Maximum number of login attempts” field (11) to define the maximum number of login attempts before the user is blocked because an incorrect password is entered
- Complete the “Lockout time for too many failed login attempts” field (12) to define the time for which a user is locked out following too many incorrect password entries
- Click on “Save and apply changes” in the “Settings” section to apply the changes

2 "PASSWORD" TAB

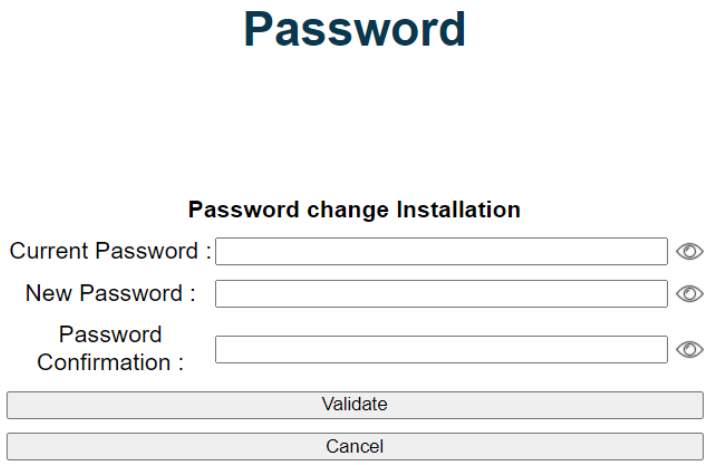

Figure 7: "Password" tab

To change the password of the web user logged in, go to the "System" page "Password" tab (Figure 7):

- Enter the current password in the "Current password" field
- Enter the new password in the "New password" field
- Enter the new password again in the "Password confirmation" field
- Click on "Confirm" to confirm the change of password or on "Cancel" to cancel

Note: The password must contain at least 8 characters, including one number, one upper case letter, one lower case letter and one special character

3 "USERS" TAB

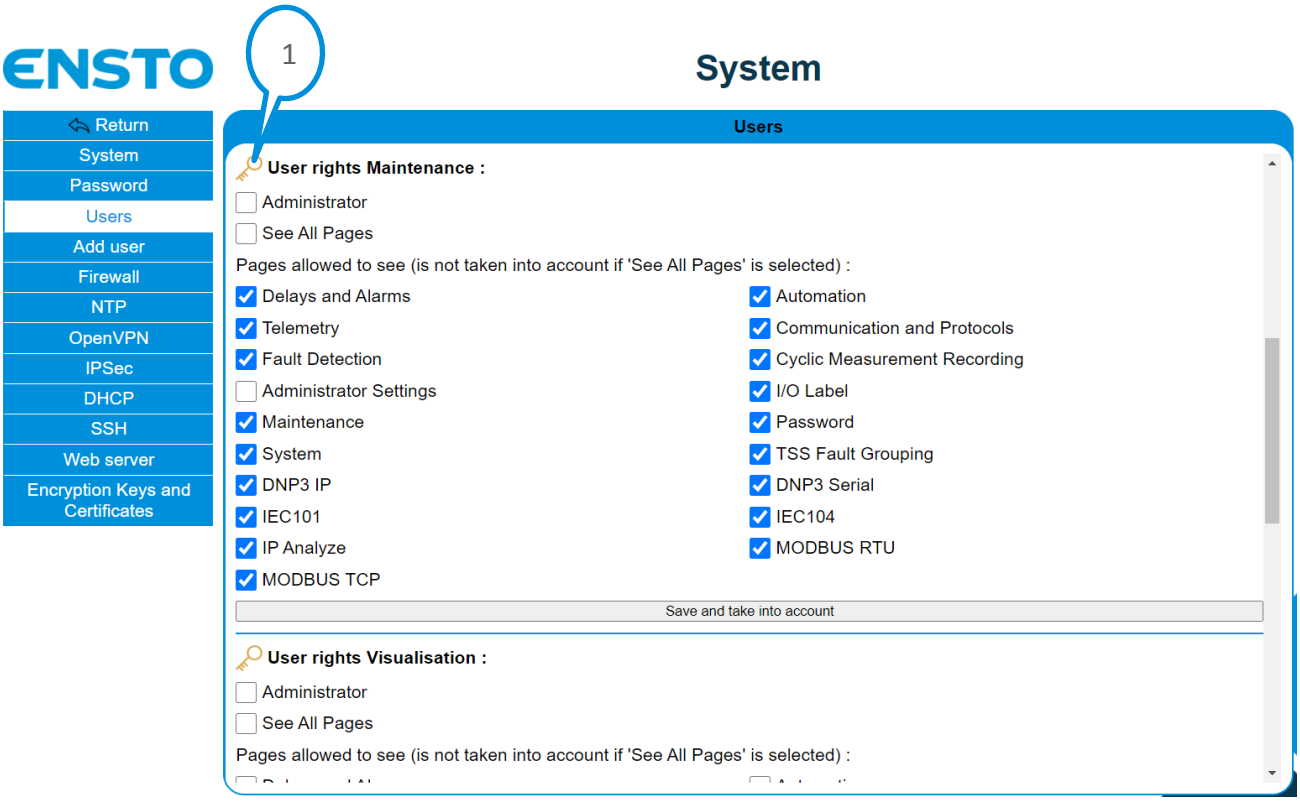

Figure 8: "Users" tab

This tab allows web users rights to be configured and their password to be changed.

To configure the rights of a web user **(for users with "Administrator" rights only)**, go to the "System" page "Users" tab (Figure 8):

- Click on the "Administrator" box for the user to have administrator rights
- Click on the "See All pages" box for the user to be able to see all the web pages
- Select the pages that the user can see in the "Pages allowed to see" section
- Click on "Save and apply" to apply the changes

Note: Rights are configured user by user

To change the password of a web user **(for users with "Administrator" rights only)**, go to the "System" page "Users" tab (Figure 8):

- Click on the key alongside the username (1)
- Depending on your internet browser, a dialog box opens
- Enter the new password
- Click on "OK" to confirm the change of password or on "Cancel" to cancel

Note: It is not possible to change the password of a user with "Administrator" rights in this way
Note: The password must contain at least 8 characters, including one number, one upper case letter, one lower case letter and one special character

4 "ADD USER" TAB

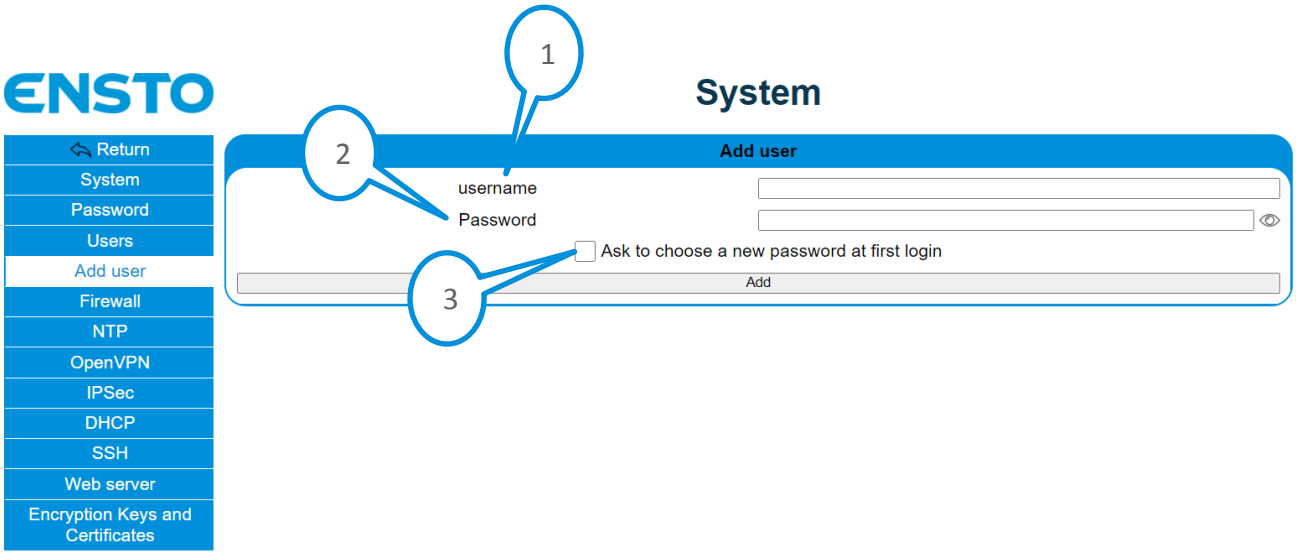

Figure 9: "Add user" tab

To add a web user **(for users with "Administrator" rights only)**, go to the "System" page "Add user" tab (Figure 9):

- Complete the "Username" field (1) with a new username
- Complete the "Password" field (2) with the new user's password
- Click on the "Request that a new password be defined on first login" box in order that, when the user logs in for the first time, he/she is asked to change his/her password
- Click on "Add" to add the new user

Note: The password does not need to comply with the following password rule: at least 8 characters, including one number, one upper case letter, one lower case letter and one special character

5 "FIREWALL" TAB

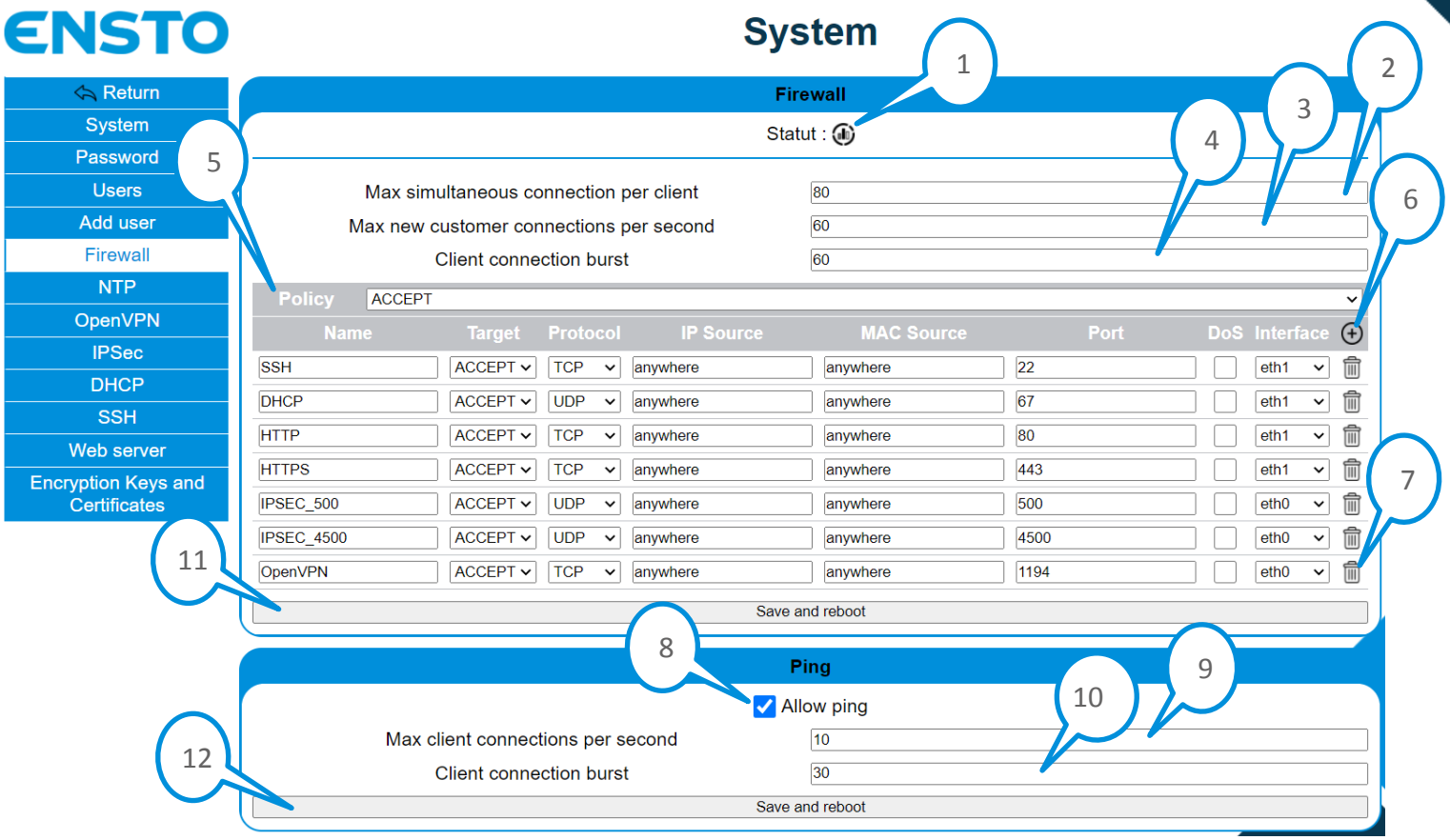

Figure 10: "Firewall" tab

5.1. FIREWALL STATUS

To display the Firewall status **(for users with "Administrator" rights only)**, go to the "System" page "Firewall" tab "Firewall" block (Figure 10):

- Click on the graphic icon (1)
- The Firewall status dialog box opens, example:

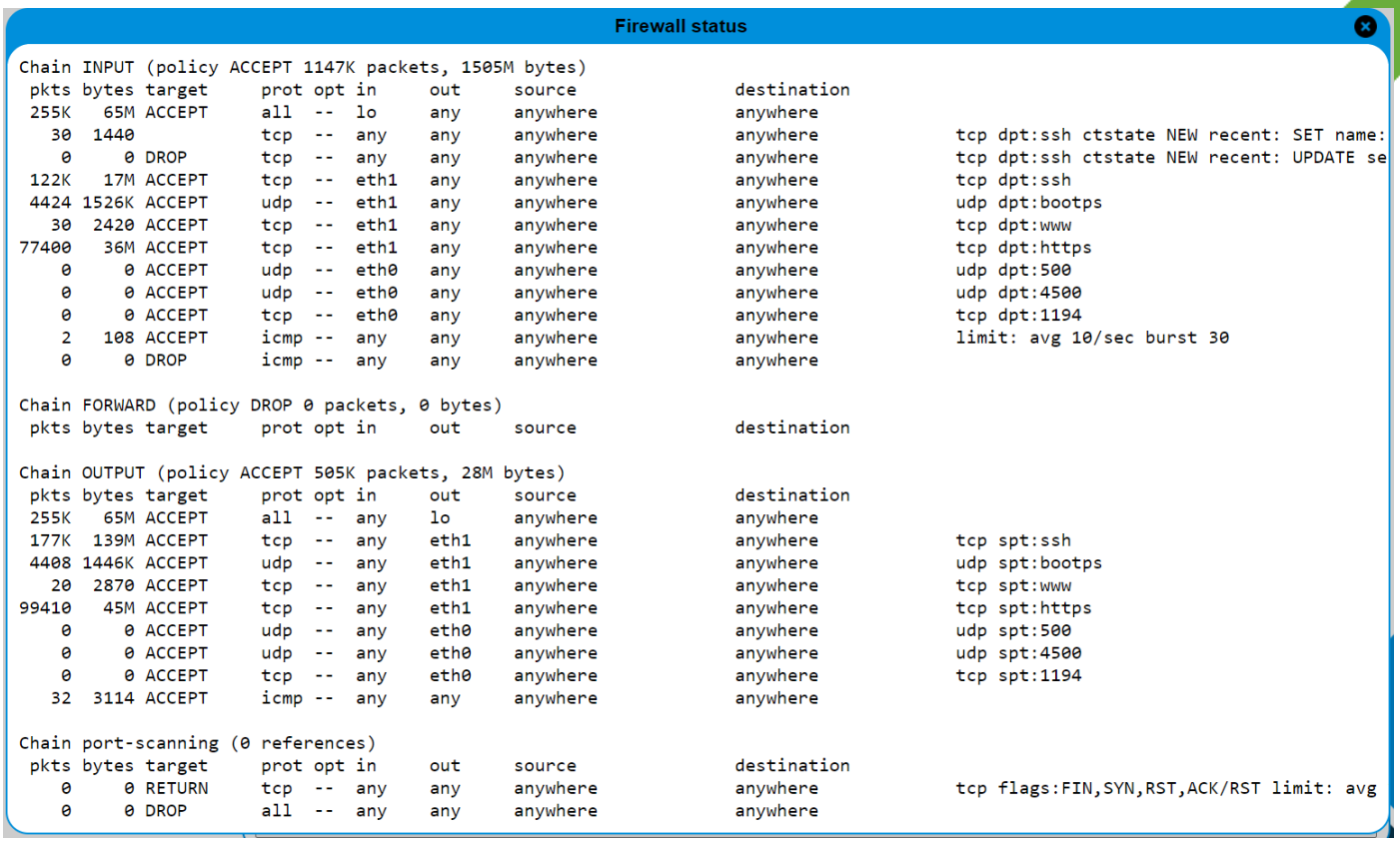

Figure 11: Firewall status dialog box

5.2. DoS (DENIAL OF SERVICE) PROTECTION CONFIGURATION

To configure the DoS protection **(for users with "Administrator" rights only)**, go to the "System" page "Firewall" tab "Firewall" block (Figure 10):

- Complete the "Max simultaneous connections per client" field (2) to define the maximum number of simultaneous TCP connections by a client
- Complete the "Max new client connections per second" field (3) to define the maximum number of new TCP connections by a client per second
- Complete the "Client connection burst" field (4) to define the number of fast TCP connections by a client
- Click on "Save and reboot" (11) to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: DoS protection must be activated for each firewall rule
Note: Attention: the activation of DoS protection may slow down TCP connection
Note: Before clicking on "Save and reboot", it is possible to configure the general rule and the specific rules for the Firewall at the same time

5.3. FIREWALL RULES CONFIGURATION

To configure the general Firewall rule **(for users with "Administrator" rights only)**, go to the "System" page "Firewall" tab "Firewall" block (Figure 10):

- Select the general rule "Policy" (5) for the Firewall: "ACCEPT" → All the IP connections are accepted except if a specific rule specifies otherwise; "DROP" → All the IP connections are rejected except if a specific rules specifies otherwise
- Click on "Save and reboot" (11) to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on "Save and reboot", it is possible to configure the DoS protection and the specific rules for the Firewall at the same time

To configure the specific Firewall rules **(for users with "Administrator" rights only)**, go to the "System" page "Firewall" tab "Firewall" block (Figure 10):

- Click on the "+" icon (6) to add a new rule
- Complete the following fields:
  - "Name" to give the rule a name (without spaces)
  - "Target" to accept (ACCEPT) or reject (DROP) the connection
  - "Protocol" to specify the type of IP connection (TCP or UDP)
  - "IP source" to accept or reject the specified IP address (by using the keyword "anywhere", which means all IP addresses)
  - "MAC source" to accept or reject the specified MAC address (by using the keyword "anywhere", which means all MAC addresses)
  - "Port" to specify the IP port accepted or rejected
  - "DoS" to activate DoS protection
  - "Interface" to specify the interface (by default, eth0 = Communication; eth1 = Configuration; eth2 = Extension)
- Click on "Save and reboot" (11) to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on "Save and reboot", it is possible to configure the DoS protection and the general rule for the Firewall at the same time

To remove a specific Firewall rule **(for users with "Administrator" rights only)**, go to the "System" page "Firewall" tab "Firewall" block (Figure 10):

- Click on the "Recycle bin" icon for the rule to be removed (example 7)
- Click on "Save and reboot" (11) to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on "Save and reboot", it is possible to configure the DoS protection and the general rule for the Firewall at the same time

5.4. PING CONFIGURATION

To allow/deny PING **(for users with "Administrator" rights only)**, go to the "System" page "Firewall" tab "Ping" block (Figure 10):

- Select or deselect the "Allow ping" box (8) to allow or deny PING
- Click on "Save and reboot" (12) to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on "Save and reboot", it is possible to configure the ICMP protection at the same time

To configure the ICMP protection **(for users with "Administrator" rights only)**, go to the "System" page "Firewall" tab "Ping" block (Figure 10):

- Complete the "Max client connections per second" (2) to define the maximum number of ICMP connections by a client per second
- Complete the "Client connection burst" field (4) to define the number of fast ICMP connections by a client
- Click on "Save and reboot" (12) to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on "Save and reboot", it is possible to configure the allowance or denial of PING at the same time

6 "NTP" TAB

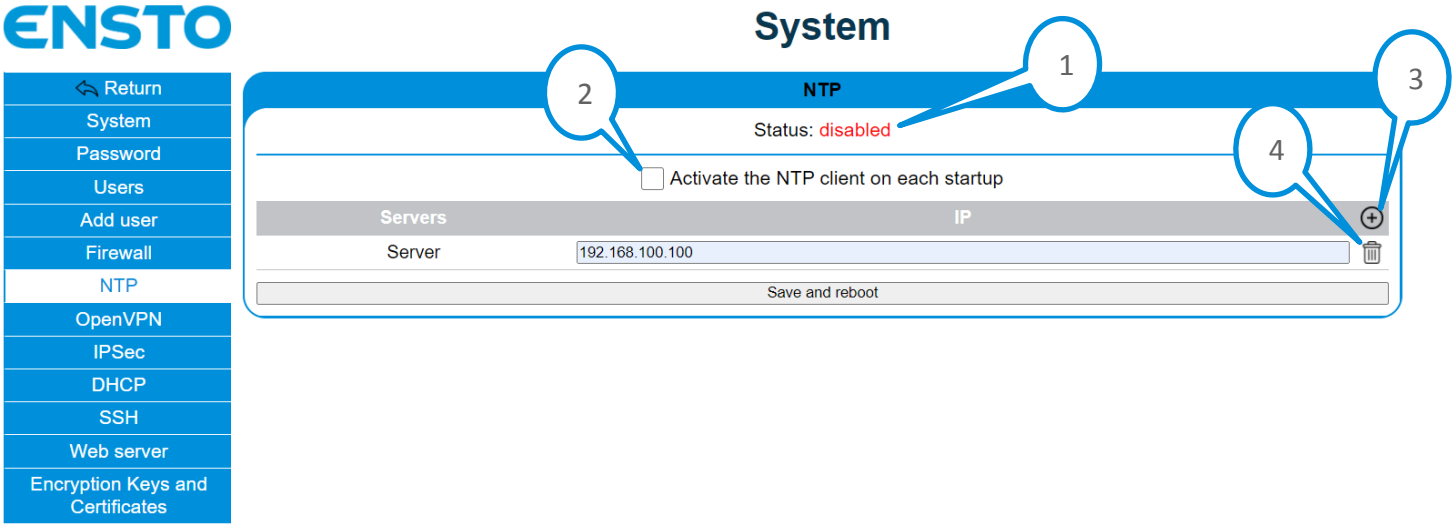

Figure 12: "NTP" tab

6.1. NTP CLIENT STATUS

To view the NTP client status (activated or deactivated) **(for users with "Administrator" rights only)**, go to the "System" page "NTP" tab (Figure 12):

- The "Status" field (1) indicates whether the NTP client is activated or deactivated

6.2. NTP CLIENT CONFIGURATION

To activate/deactivate the NTP client **(for users with "Administrator" rights only)**, go to the "System" page "NTP" tab (Figure 12):

- Select or deselect the "Activate the NTP client on each startup" box (2) to activate or deactivate the NTP client
- Click on "Save and reboot" to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on "Save and reboot", it is possible to configure the NTP servers at the same time

To add an NTP server **(for users with "Administrator" rights only)**, go to the "System" page "NTP" tab (Figure 12):

- Click on the "+" icon (3) to add a server
- Complete the "IP" field to specify the IP address of the NTP server
- Click on "Save and reboot" to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on "Save and reboot", it is possible to configure the activation or deactivation of the NTP client at the same time

To remove an NTP server **(for users with "Administrator" rights only)**, go to the "System" page "NTP" tab (Figure 12):

- Click on the "Recycle bin" icon for the server to be removed (example 4)
- Click on "Save and reboot" to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on "Save and reboot", it is possible to configure the activation or deactivation of the NTP client at the same time

7 "OPENVPN" TAB

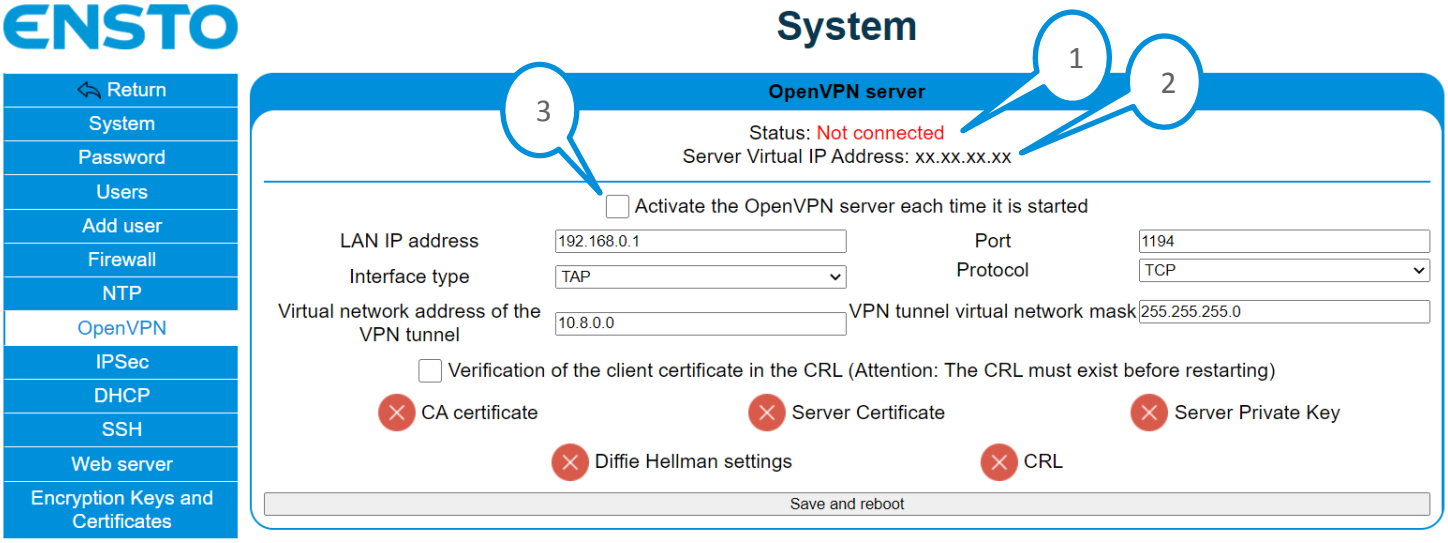

Figure 13: "OpenVPN" tab

7.1. OPENVPN SERVER STATUS

To view the OpenVPN server status **(for users with "Administrator" rights only)**, go to the "System" page "OpenVPN" tab (Figure 13):

- The "Status" field (1) indicates whether the OpenVPN server is activated or deactivated
- The "Server Virtual IP Address" field (2) indicates the virtual IP address of the OpenVPN server when it is connected

Note: The virtual IP address of the server is the IP address with which it must communicate to pass through the VPN tunnel

7.2. OPENVPN SERVER CONFIGURATION

To activate/deactivate the OpenVPN server **(for users with "Administrator" rights only)**, go to the "System" page "OpenVPN" tab (Figure 13):

- Select or deselect the "Activate the OpenVPN server on each startup" box (3) to activate or deactivate the OpenVPN server
- Click on "Save and reboot" to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on "Save and reboot", it is possible to configure the OpenVPN server at the same time

To configure the OpenVPN server **(for users with "Administrator" rights only)**, go to the "System" page "OpenVPN" tab (Figure 13):

- Complete the "LAN IP address" field to specify the IP address of the cabinet interface via which the VPN must pass. Example, if the IP address for eth0 (COM) is 192.168.0.1, this field must be completed with this address
- Complete the "Port" field to specify the server's TCP or UDP port

- Complete the “Interface type” field to specify the interface type (TAP or TUN)
- Complete the “Protocol” field to specify the type of protocol (TCP or UDP)
- Complete the “Virtual network address of the VPN tunnel” field to specify the base address of the virtual network for the VPN tunnel
- Complete the “VPN tunnel virtual network mask” field to specify the virtual network mask for the VPN tunnel
- Select or deselect the “Verification of the client certificate in the CRL” box to activate or deactivate verification of client certificates in the CRL when connecting to the server
- Click on “Save and reboot” to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: In the example in Figure 13, the virtual network address of the tunnel is 10.8.0.0 and the mask is 255.255.255.0, therefore, the server will have the address 10.8.0.1 and a client will be assigned the address 10.8.0.10
Note: Attention: if verification of the client certificate in the CRL is activated, the CRL must be present in the cabinet before saving
Note: Before clicking on “Save and reboot”, it is possible to configure the activation or deactivation of the OpenVPN server at the same time
Note: The  *and*  *icons indicate whether the corresponding files are present in the cabinet or not. These files are added in the “Encryption Keys and Certificates” tab*

8 "IPSEC" TAB

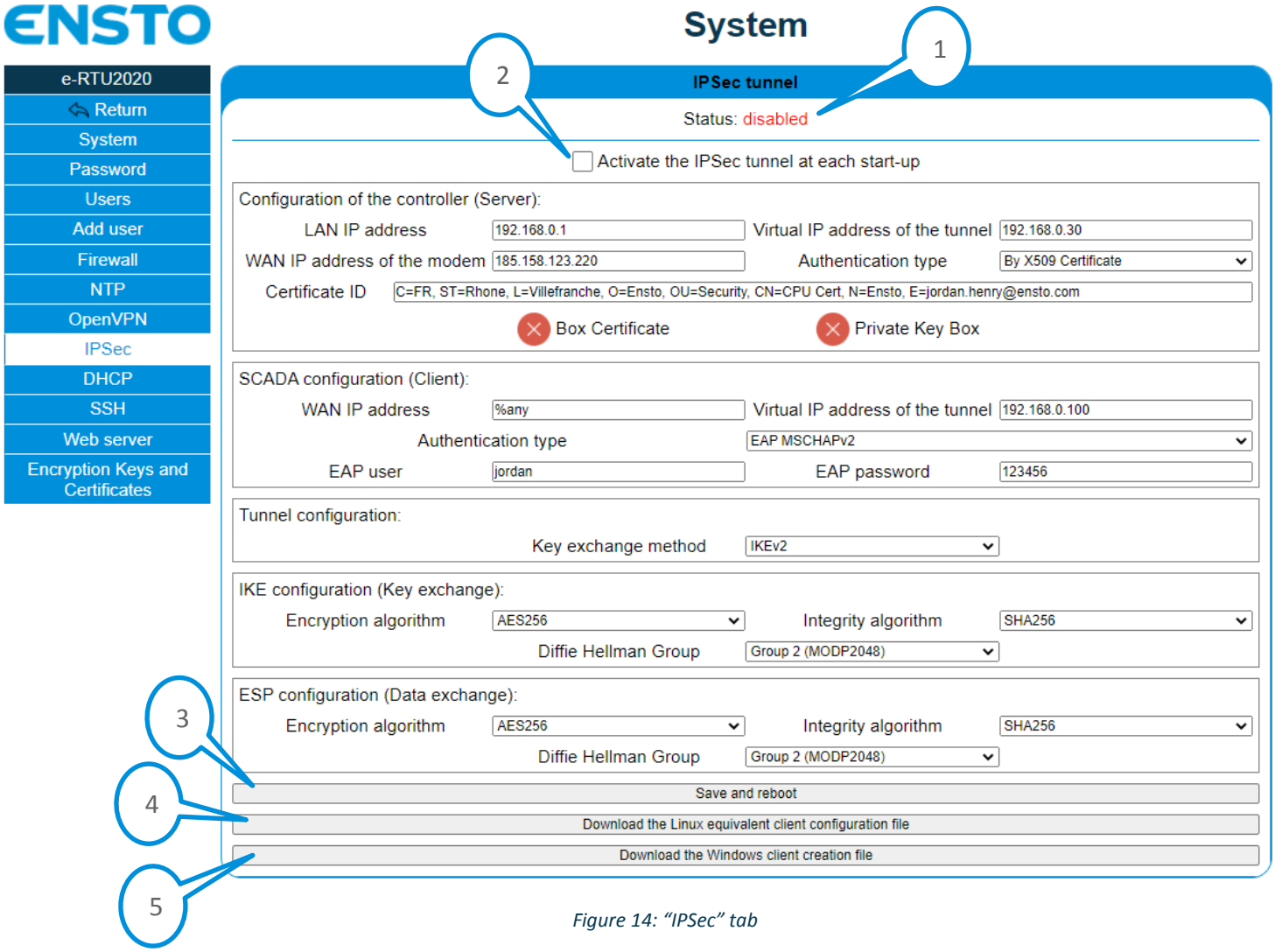

Figure 14: "IPSec" tab

8.1 IPSEC TUNNEL STATUS

To view the IPSec tunnel status (activated or deactivated) **(for users with "Administrator" rights only)**, go to the "System" page "IPSec" tab (Figure 14):

- The "Status" tab (1) indicates whether the IPSec tunnel is activated or deactivated

8.2 IPSEC TUNNEL CONFIGURATION

To activate/deactivate the IPSec tunnel **(for users with "Administrator" rights only)**, go to the "System" page "IPSec" tab (Figure 14):

- Select or deselect the “Activate the IPSec tunnel on each startup” box (2) to activate or deactivate the IPSec tunnel
- Click on “Save and reboot” (3) to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on “Save and reboot” it is possible to configure the IPSec tunnel at the same time

To configure the IPSec tunnel **(for users with “Administrator” rights only)**, go to the “System” page “IPSec” tab (Figure 14):

- Configure the cabinet side (server):
  - Complete the “LAN IP address” field to specify the IP address of the cabinet interface via which the VPN must pass. Example, if the IP address for eth0 (COM) is 192.168.0.1, this field must be completed with this address
  - Complete the “Virtual IP address of the tunnel” field to specify the virtual IP address that the cabinet will use to communicate via the VPN tunnel
  - Complete the “WAN IP address of the modem” to specify the WAN IP address if the cabinet is connected to a modem (IP radio or GPRS or other) otherwise leave it blank
  - Complete the “Authentication type” field to specify the type of authentication for the cabinet to the SCADA system
  - Complete the “Certificate ID” field to specify the ID present in the X.509 certificate, which is used to authenticate the cabinet to the SCADA system
- Configuration of the SCADA side (client):
  - Complete the “WAN IP address” field to specify the WAN IP address of the SCADA system, which will connect to the cabinet (by entering the keyword “%any”, which means all IP addresses)
  - Complete the “Virtual IP address of the tunnel” field to specify the virtual IP address that the SCADA system will use to communicate via the VPN tunnel
  - Complete the “Authentication type” field to specify the type of authentication for the SCADA system to the cabinet
  - Complete the “EAP user” field to specify the username for authentication of the SCADA system to the cabinet
  - Complete the “EAP password” field to specify the password for authentication of the SCADA system to the cabinet
- Tunnel configuration:
  - Complete the “Key exchange method” field to specify the method for exchanging keys
- IKE configuration (Key exchange):
  - Complete the “Encryption algorithm” field to specify the type of encryption algorithm
  - Complete the “Integrity algorithm” field to specify the type of integrity algorithm
  - Complete the “Diffie-Hellman Group” field to specify the Diffie-Hellman group
- ESP configuration (Data exchange):
  - Complete the “Encryption algorithm” field to specify the type of encryption algorithm

- Complete the “Integrity algorithm” field to specify the type of integrity algorithm
- Complete the “Diffie-Hellman Group” field to specify the Diffie-Hellman group

- Click on “Save and reboot” (3) to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on “Save and reboot”, it is possible to configure the activation or deactivation of the IPSec tunnel at the same time
Note: The and icons indicate whether the corresponding files are present in the cabinet or not. These files are added in the “Encryption Keys and Certificates” tab

To download the corresponding Windows or Linux client configuration files for server configuration **(for users with “Administrator” rights only)**, go to the “System” page “IPSec” tab (Figure 14):

- Click on “Download the Linux equivalent client configuration file” to download the client configuration file for Linux
- Click on “Download the Windows client creation file” to download the Windows client configuration file. This file contains PowerShell commands, you need to open a PowerShell terminal with Administrator rights and run the commands to create the IPSec client

9 "DHCP" TAB

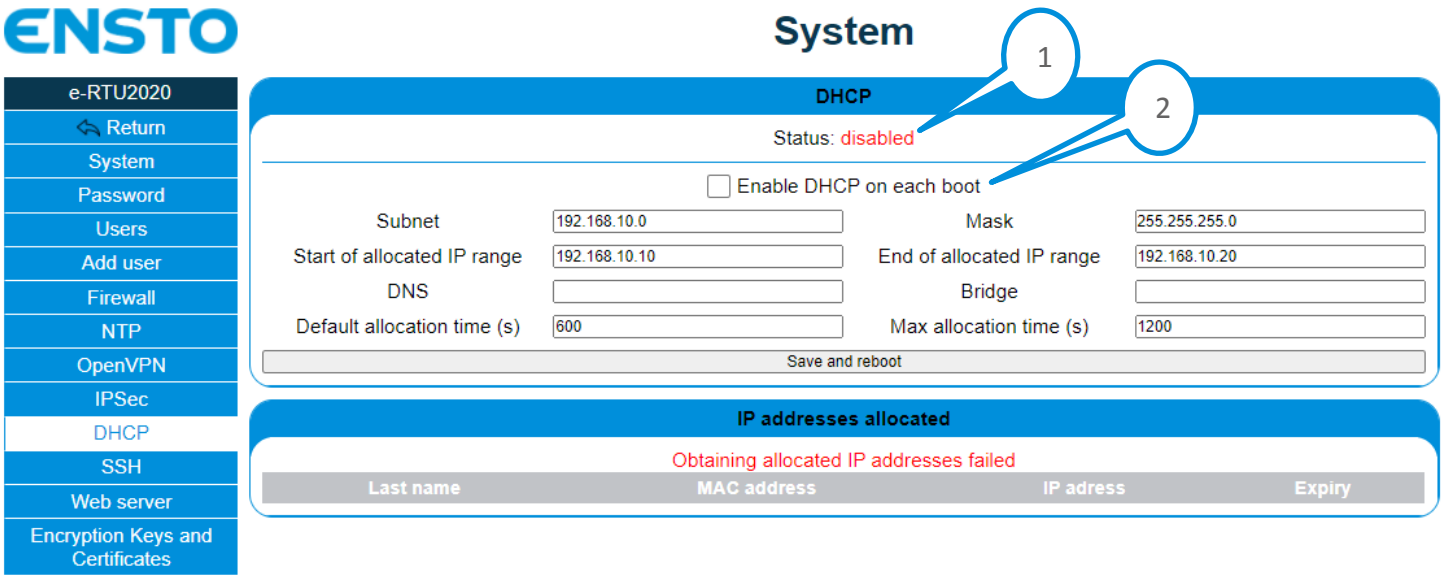

Figure 15: "DHCP" tab

9.1. DHCP SERVER STATUS

To view the DHCP status (activated or deactivated) **(for users with "Administrator" rights only)**, go to the "System" page "DHCP" tab "DHCP" block (Figure 15):

- The "Status" field (1) indicates whether the DHCP server is activated or deactivated

9.2. DHCP SERVER CONFIGURATION

To activate/deactivate the DHCP **(for users with "Administrator" rights only)**, go to the "System" page "DHCP" tab "DHCP" block (Figure 15):

- Select or deselect the "Activate the DHCP on each startup" box (2) to activate or deactivate the DHCP server
- Click on "Save and reboot" to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on "Save and reboot", it is possible to configure the DHCP server at the same time

To configure the DHCP server **(for users with "Administrator" rights only)**, go to the "System" page "DHCP" tab "DHCP" block (Figure 15):

- Complete the "Subnet" field to specify the subnet in which the IP addresses will be allocated. Must correspond to the eth1 interface (Configuration)
- Complete the "Mask" field to specify the subnet mask
- Complete the "Start of allocated IP range" field to specify the start of the range of allocated IP addresses
- Complete the "End of allocated IP range" field to specify the end of the range of allocated IP addresses
- (Optional) Complete the "DNS" field to specify the IP address of the DNS server

- (Optional) Complete the “Gateway” field to specify the IP address of the gateway
- Complete the “Default allocation time (s)” field to specify the default allocation time for an IP address
- Complete the “Max allocation time (s)” field to specify the maximum allocation time for an IP address
- Click on “Save and reboot” (3) to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on “Save and reboot”, it is possible to configure the activation or deactivation of the DHCP server at the same time

9.3. IP ADDRESSES ALLOCATED

To view the IP addresses allocated by the DHCP server **(for users with “Administrator” rights only)**, go to the “System” page “DHCP” tab “IP addresses allocated” block (Figure 15):

- The “Name” field corresponds to the name of the client connected to the server
- The “MAC address” field corresponds to the MAC address of the client connected to the server
- The “IP address” field corresponds to the IP address of the client that the server has allocated
- The “Expiry” field corresponds to the expiry date for the client IP address before renegotiation

10 "SSH" TAB

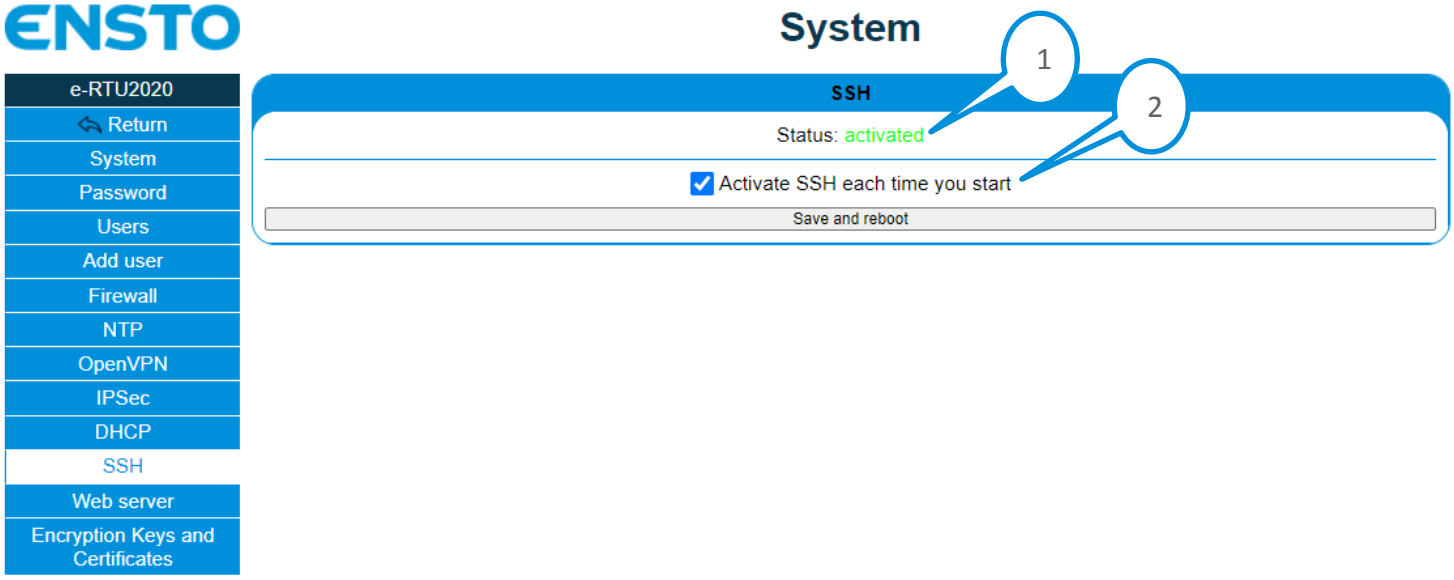

Figure 16: "SSH" tab

10.1. SSH SERVER STATUS

To view the SSH server status (activated or deactivated) **(for users with "Administrator" rights only)**, go to the "System" page "SSH" tab (Figure 16):

- The "Status" field (1) indicates whether the SSH is activated or deactivated

10.2. SSH SERVER CONFIGURATION

To activate/deactivate the SSH server **(for users with "Administrator" rights only)**, go to the "System" page "SSH" tab (Figure 16):

- Select or deselect the "Activate SSH on each startup" box (2) to activate or deactivate the SSH
- Click on "Save and reboot" to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears

11 "WEB SERVER" TAB

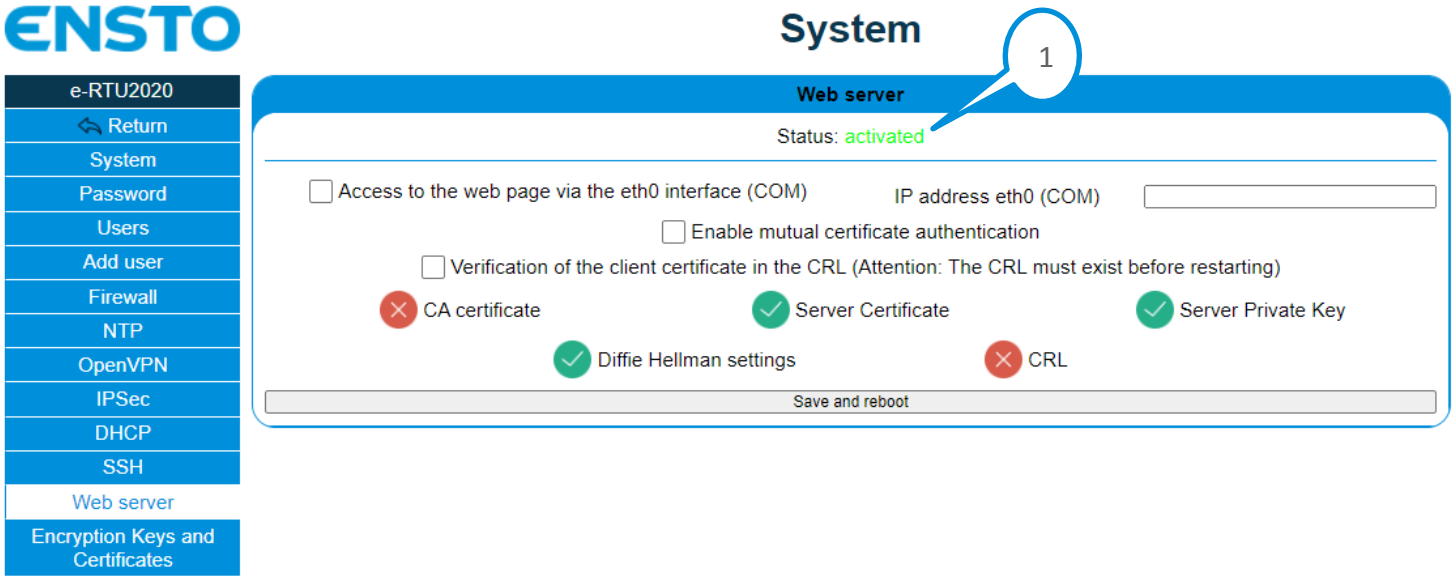

Figure 17: "Web server" tab

11.1. WEB SERVER STATUS

To view the Web server status (activated or deactivated) **(for users with "Administrator" rights only)**, go to the "System" page "Web server" tab (Figure 17):

- The "Status" field (1) indicates whether the Web server is activated or deactivated

11.2. WEB SERVER CONFIGURATION

To activate or deactivate Web server remote access **(for users with "Administrator" rights only)**, go to the "System" page "Web server" tab (Figure 17):

- Select or deselect the "Access to the Web page via the eth0 interface (COM)" box to activate or deactivate remote access
- Complete the "IP address eth0 (COM)" field with the IP address of the Ethernet interface eth0 (COM)
- Click on "Save and reboot" to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on "Save and reboot" ,it is possible to configure the other Web server functions

To activate or deactivate mutual authentication **(for users with "Administrator" rights only)**, go to the "System" page "Web server" tab (Figure 17):

- Select or deselect the "Enable mutual certificate authentication" box to activate or deactivate mutual authentication
- Select or deselect the "Verification of the client certificate in the CRL" box to activate or deactivate verification of client certificates in the CRL when connecting to the server

- Click on “Save and reboot” to apply the changes
- Wait for the cabinet to reboot

Note: The reboot is complete when the web server connection page appears
Note: Before clicking on “Save and reboot” ,it is possible to configure the other Web server functions
Note: Attention: if verification of the client certificate in the CRL is activated, the CRL must be present in the cabinet before saving
Note: Mutual authentication obliges the client to identify itself to the Web server with a certificate
Note: The and icons indicate whether the corresponding files are present in the cabinet or not. These files are added in the “Encryption Keys and Certificates” tab

12 "ENCRYPTION KEYS AND CERTIFICATES" TAB

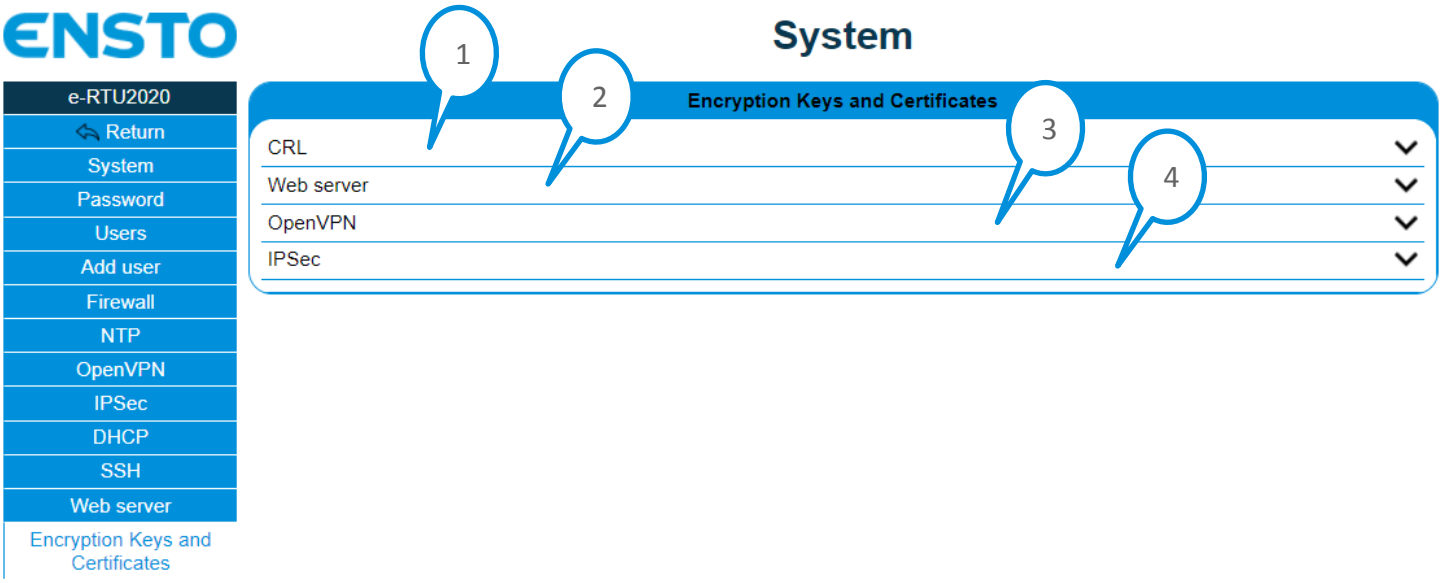

Figure 18: "Encryption Keys and Certificates" tab

12.1. CRL

To configure the CRL **(for users with "Administrator" rights only)**, go to the "System" page "Encryption Keys and Certificates" tab (Figure 18):

- Click on the "CRL" pane (1)
- The CRL configuration pane opens:

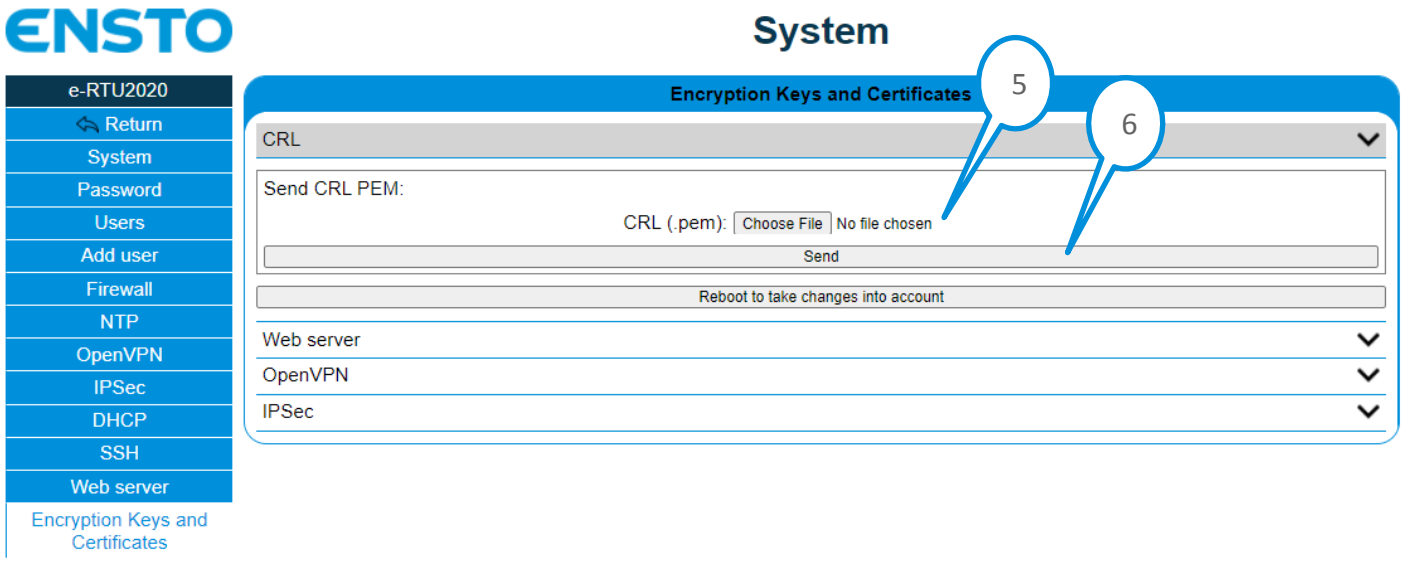

Figure 19: CRL configuration pane

- Click on “Select a file” (5)
- Depending on your internet browser, a dialog box opens
- Select the PEM file encoded in base 64 corresponding to the CRL
- Click on “Send” (6) to transfer the CRL

Note: After pressing “Send”, the CRL is uploaded to the cabinet but is not applied, the cabinet must be rebooted for it to be applied by pressing “Reboot to apply changes”

12.2. WEB SERVER

To configure the Web server keys and certificates **(for users with “Administrator” rights only)**, go to the “System” page “Encryption Keys and Certificates” tab (Figure 18):

- Click on the “Web server” pane (2)
- The Web server keys and certificates configuration pane opens:

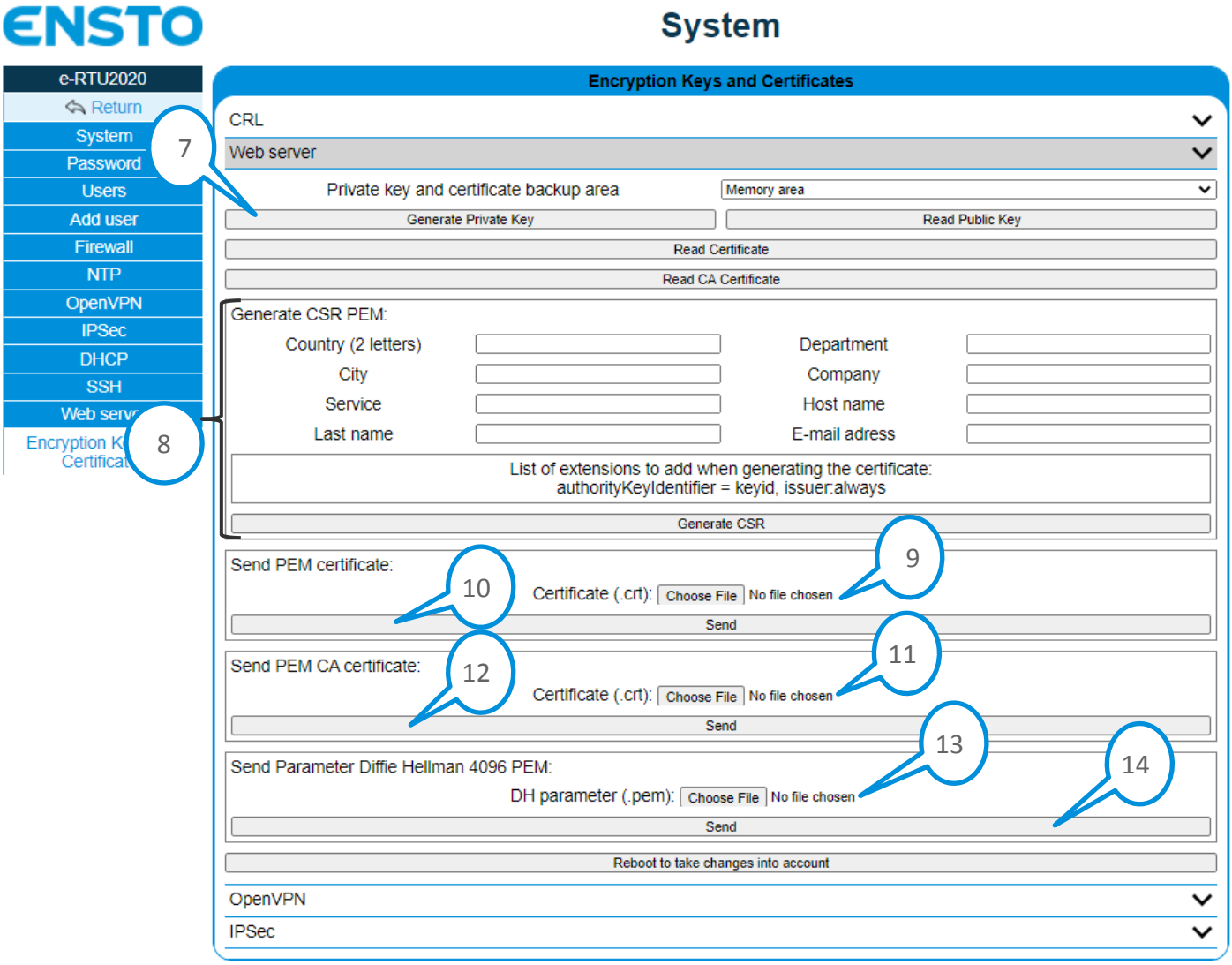

Figure 20: Web server keys and certificates configuration pane

- Click on “Generate Private Key” (7) to generate the private key for the Web server
- Generate the certificate signing request (CSR) for the Web server (8):
  - Complete the “Country (2 letters)” field to specify the 2 country letters for the certificate (example: FR)
  - Complete the “Department” field to specify the *département* for the certificate (example: Rhône)
  - Complete the “City” field to specify the city for the certificate (example: Lyon)
  - Complete the “Company” field to specify the company for the certificate (example: Ensto)
  - Complete the “Service” field to specify the division for the certificate (example: Security)
  - Complete the “Host name” field to specify the name of the host for the certificate (example: Ensto)
  - Complete the “Name” field to specify the name for the certificate (example: Web certificate)
  - Complete the “E-mail address” field to specify the e-mail address for the certificate (example: security@ensto.com)
  - Click on “Generate CSR” to generate and download the CSR in PEM format encoded in base 64
  - Depending on your internet browser, the file is downloaded
- Send the signing request to a certification authority of your choice in order to generate the Web server certificate
- Transfer the Web server certificate:
  - Click on “Select a file” (9)
  - Depending on your internet browser, a dialog box opens
  - Select the CRT file encoded in base 64 corresponding to the Web server certificate
  - Click on “Send” (10) to transfer the certificate
- Transfer the certification authority certificate:
  - Click on “Select a file” (11)
  - Depending on your internet browser, a dialog box opens
  - Select the CRT file encoded in base 64 corresponding to the certification authority certificate
  - Click on “Send” (12) to transfer the certificate
- Transfer the Diffie-Hellman parameter:
  - Generate a PEM file encoded in base 64 containing a Diffie-Hellman parameter of 4096 bits → It is possible to generate this parameter using the “openSSL” tool in Linux with the “openSSL dhparam -out dhparam.pem 4096” command
  - Click on “Select a file” (13)
  - Depending on your internet browser, a dialog box opens
  - Select the PEM file encoded in base 64 corresponding to the Diffie-Hellman parameter
  - Click on “Send” (14) to transfer the certificate

Note: When a new private key is generated, a new certificate must also be generated in order that it corresponds to this new key
Note: Once all the files have been transferred to the cabinet, the latter must be rebooted in order for them to be applied by pressing “Reboot to apply changes”

12.3. OPENVPN

To configure the OpenVPN server keys and certificates **(for users with "Administrator" rights only)**, go to the "System" page "Encryption Keys and Certificates" tab (Figure 18):

- Click on the "OpenVPN" pane (3)
- The OpenVPN server keys and certificates configuration pane opens:

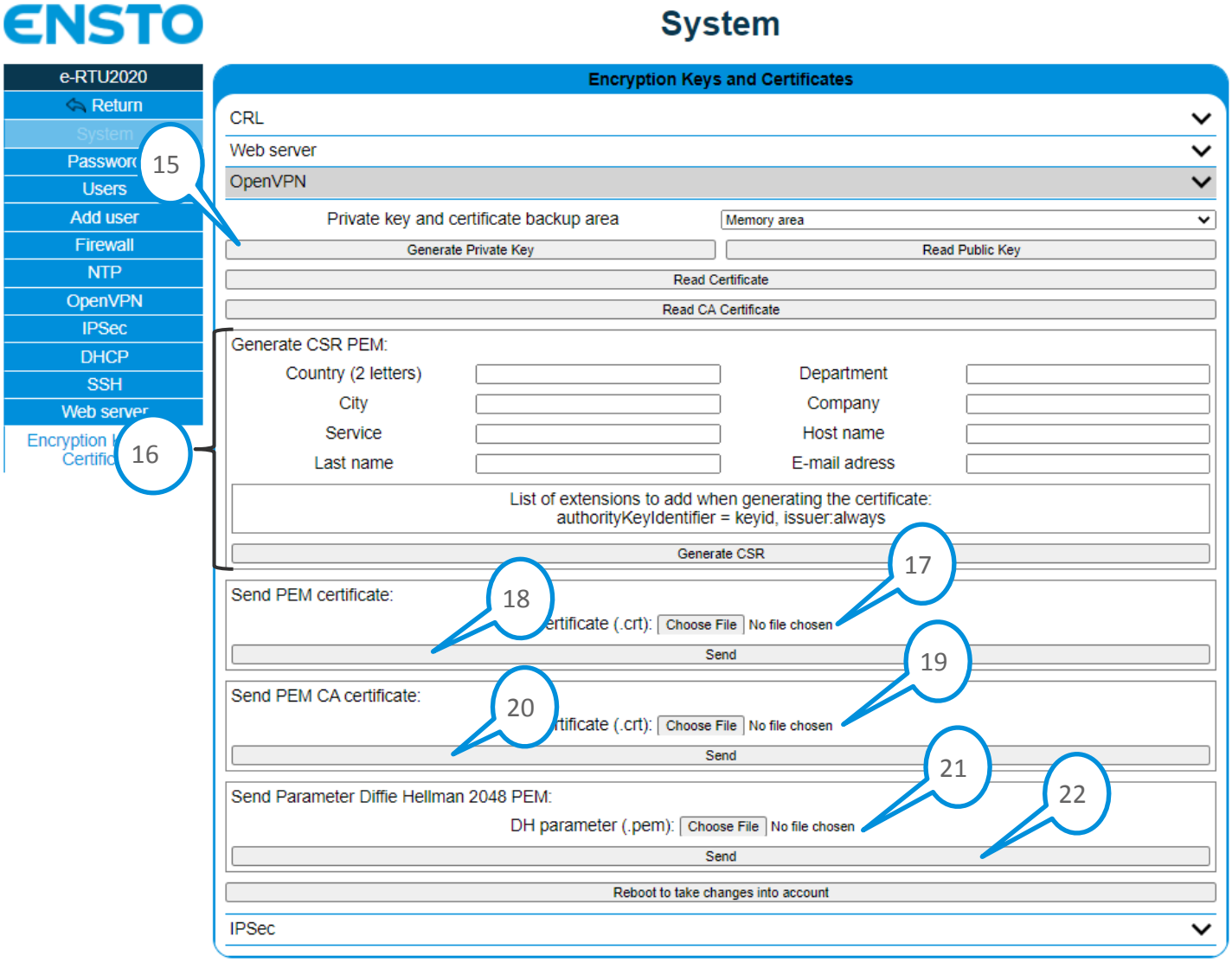

Figure 21: OpenVPN server keys and certificates configuration pane

- Click on "Generate Private Key" (15) to generate the private key for the OpenVPN server
- Generate the certificate signing request (CSR) for the OpenVPN server (16):
  - Complete the "Country (2 letters)" field to specify the 2 country letters for the certificate (example: FR)
  - Complete the "Department" field to specify the *département* for the certificate (example: Rhône)
  - Complete the "City" field to specify the city for the certificate (example: Lyon)
  - Complete the "Company" field to specify the company for the certificate (example: Ensto)

- Complete the “Service” field to specify the division for the certificate (example: Security)
- Complete the “Host name” field to specify the name of the host for the certificate (example: Ensto)
- Complete the “Name” field to specify the name for the certificate (example: OpenVPN Server Certificate)
- Complete the “E-mail address” field to specify the e-mail address for the certificate (example: security@ensto.com)
- Click on “Generate CSR” to generate and download the CSR in PEM format encoded in base 64
- Depending on your internet browser, the file is downloaded

- Send the signing request to a certification authority of your choice in order to generate the OpenVPN server certificate
- Transfer the OpenVPN server certificate:
  - Click on “Select a file” (17)
  - Depending on your internet browser, a dialog box opens
  - Select the CRT file encoded in base 64 corresponding to the OpenVPN server certificate
  - Click on “Send” (18) to transfer the certificate
- Transfer the certification authority certificate:
  - Click on “Select a file” (19)
  - Depending on your internet browser, a dialog box opens
  - Select the CRT file encoded in base 64 corresponding to the certification authority certificate
  - Click on “Send” (20) to transfer the certificate
- Transfer the Diffie-Hellman parameter:
  - Generate a PEM file encoded in base 64 containing a Diffie-Hellman parameter of 2048 bits → It is possible to generate this parameter using the “openSSL” tool in Linux with the “openSSL dhparam -out dh2048.pem 2048” command
  - Click on “Select a file” (21)
  - Depending on your internet browser, a dialog box opens
  - Select the PEM file encoded in base 64 corresponding to the Diffie-Hellman parameter
  - Click on “Send” (22) to transfer the certificate

Note: When a new private key is generated, a new certificate must also be generated in order that it corresponds to this new key
Note: Once all the files have been transferred to the cabinet, the latter must be rebooted in order for them to be applied by pressing “Reboot to apply changes”

12.4. IPSec

To configure the IPSec server keys and certificates **(for users with “Administrator” rights only)**, go to the “System” page “Encryption Keys and Certificates” tab (Figure 18):

- Click on the “IPSec” pane (4)
- The IPSec server keys and certificates configuration pane opens:

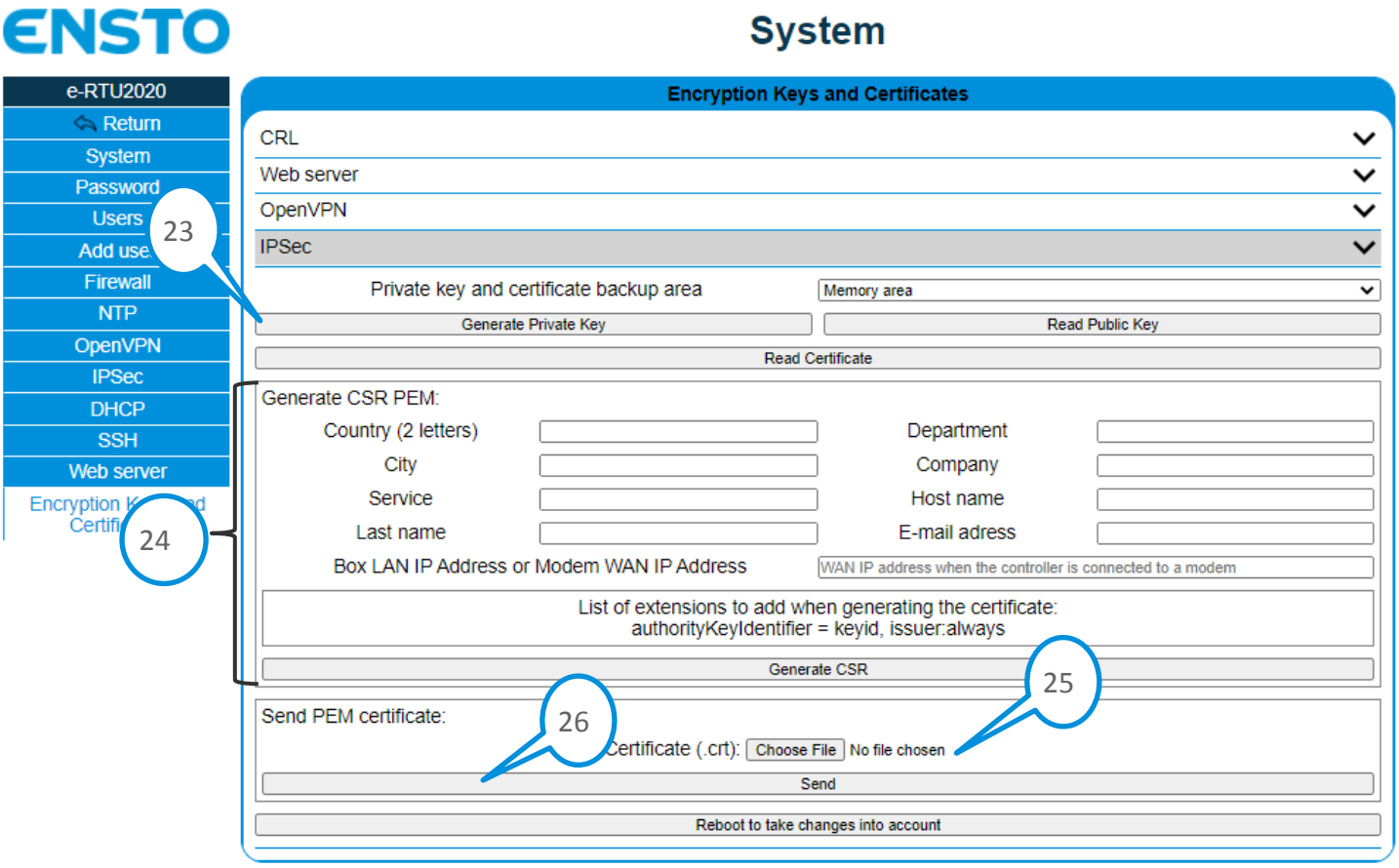

Figure 22: IPSec server keys and certificates configuration pane

- Click on “Generate Private Key” (23) to generate the private key for the IPSec server
- Generate the certificate signing request (CSR) for the IPSec server (24):
  - Complete the “Country (2 letters)” field to specify the 2 country letters for the certificate (example: FR)
  - Complete the “Department” field to specify the *département* for the certificate (example: Rhône)
  - Complete the “City” field to specify the city for the certificate (example: Lyon)
  - Complete the “Company” field to specify the company for the certificate (example: Ensto)
  - Complete the “Service” field to specify the division for the certificate (example: Security)
  - Complete the “Host name” field to specify the name of the host for the certificate (example: Ensto)
  - Complete the “Name” field to specify the name for the certificate (example: IPSec Server Certificate)
  - Complete the “E-mail address” field to specify the e-mail address for the certificate (example: security@ensto.com)
  - If the cabinet is connected to a modem (IP radio or GPRS or other), complete the “Cabinet LAN IP Address or Modem WAN IP Address” field to specify the WAN IP address of the modem
  - If the cabinet is connected locally, complete the “Cabinet LAN IP Address or Modem WAN IP Address” field to specify the IP address eth0 (COM) for the cabinet

- Click on “Generate CSR” to generate and download the CSR in PEM format encoded in base 64
- Depending on your internet browser, the file is downloaded

- Send the signing request to a certification authority of your choice in order to generate the IPSec server certificate
- Transfer the IPSec server certificate:
  - Click on “Select a file” (25)
  - Depending on your internet browser, a dialog box opens
  - Select the CRT file encoded in base 64 corresponding to the IPSec server certificate
  - Click on “Send” (26) to transfer the certificate

Note: When a new private key is generated, a new certificate must also be generated in order that it corresponds to this new key
Note: Once all the files have been transferred to the cabinet, the latter must be rebooted in order for them to be applied by pressing “Reboot to apply changes”

Note

Equipment return tracking form

Service Après-Ventes /
After-Sales Service
210, rue Léon Jouhaux – BP 10446
FR – 69656 Villefranche-sur-Saône
Cedex
Landline: +33 (0)4 74 65 61 60
Mobile: +33 (0)6 08 93 26 31