Remote Access System for STAM-2 Monitoring Station

STAM-VIEW

Installation Manual

stam-view_i_en 10/11

SATEL sp. z o.o.
ul. Schuberta 79
80-172 Gdańsk
POLAND
tel. + 48 58 320 94 00
info@satel.pl
www.satel.eu

The SATEL's goal is to continually upgrade the quality of its products, which may result in alterations of their technical specifications and firmware. The current information on the introduced modifications is available on our website.
Please visit us at:
http://www.satel.eu

The purpose of the STAM-VIEW system is to expand the functionality of the STAM-2 monitoring station. It enhances the offer aimed at the station subscribers, allowing them to get access through a web browser to events and video sequences coming from the monitored premises. This solution is an extra aid for the customers of alarm monitoring and security companies. At the same time it facilitates the work of the monitoring station operators, who no longer need to engage in providing information about the status of premises. The system is distributed in the form of a virtual machine based on the VMware technology.

1. Features

- Access to the system via a web browser.
- Remote events viewing.
- Remote verification of the premises status.
- Viewing the video sequences sent by the Viver unit.
- Easy testing of the system communication at startup and periodic maintenance.
- Events filtering.
- Encrypted transmission.
- Users' and installers' permissions defined by the administrator.
- Internal messaging between users.
- Ability to make backup copy of system settings.
- Independent database.

2. System installation

The STAM-VIEW runs on the VMware ESXi system, for the management and administration of which the VMware vSphere Client program must be used. Both programs should be downloaded from the manufacturer's website http://downloads.vmware.com/.

The VMware software is an application which enables virtualization of multiple operating systems on one physical machine. The operating systems running as virtual ones can communicate with each other via Internet protocols. Such a solution saves space, reduces the cost of purchasing new equipment, and cuts down the power and cooling costs. It also increases availability of the application and ensures a high level of data protection.

2.1 Network requirements

- Local network in the address class 192.168.1.0/24 (addresses from 192.168.1.1 - 192.168.1.254 range, netmask 255.255.255.0).
- The monitoring station with which the STAM-VIEW communicates should have an IP address in the same subnet.
- 2 free IP addresses: one for the STAM-VIEW virtual machine - 192.168.1.123, the other (any one) for the VMware ESXi system.
- Router with the LAN IP address 192.168.1.1, suitably configured to redirect the https (443) port to the address 192.168.1.123, so that the service can be available via the Internet (installation of the router is required, if there is no free 192.168.1.123 IP address).

2.2 Minimum hardware requirements for the server on which VMware ESXi system is to be installed

- 64-bit processor from the family:
  Intel Xeon, series: 3000/3200, 3100/3300, 5100/5300, 5200/5400, 7100/7300, 7200/7400,
  Intel Nehalem,
  AMD Opteron.
- 2 GB RAM memory (**4 GB RAM recommended**).
- 1GB or 10GB network card (**Intel Pro 1000 recommended**).
- One or more SCSI controllers (**e.g. Adaptec 2405**).
- Storage Array (configured in RAID 1).

Note: *The hardware on which the VMware ESXi system will be installed must be included in the list available at the http://www.vmware.com/resources/compatibility/search.php web page.*

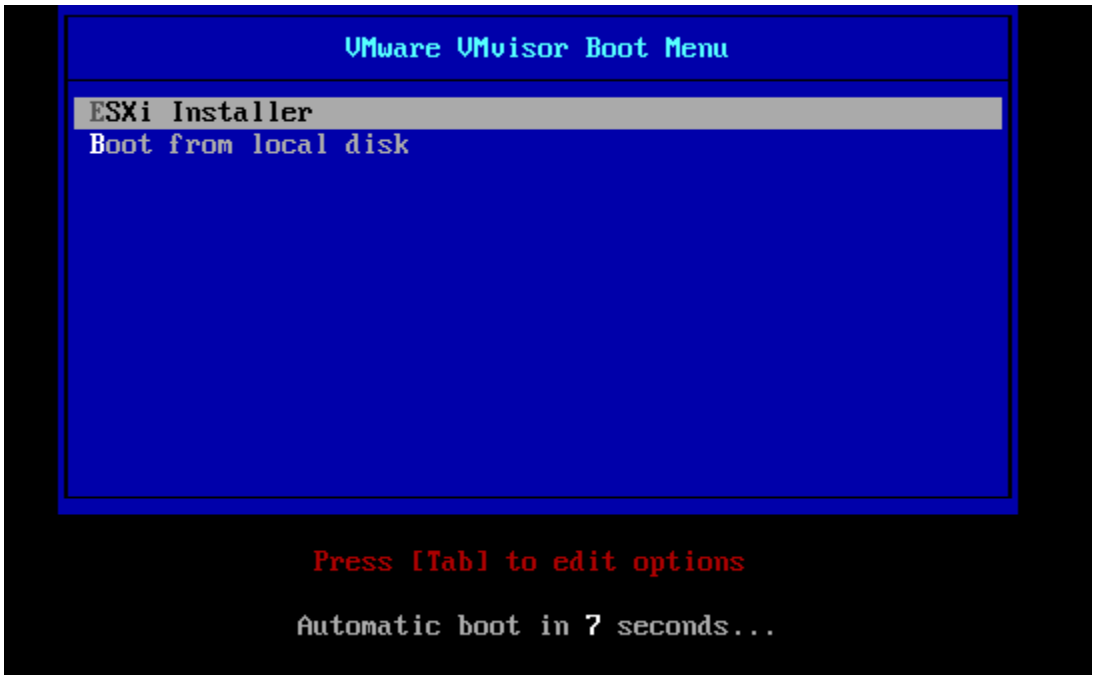
2.3 Downloading files

Open the manufacturer's website at http://downloads.vmware.com/, select the VMware vSphere Hypervisor (ESXi) item and click on the "Download" button. A page for database registration (enrollment) will be displayed. The registration is required for free downloading of files and getting of a free license for the VMware ESXi system and VMware vSphere Client program. Next, follow the manufacturer's instructions.

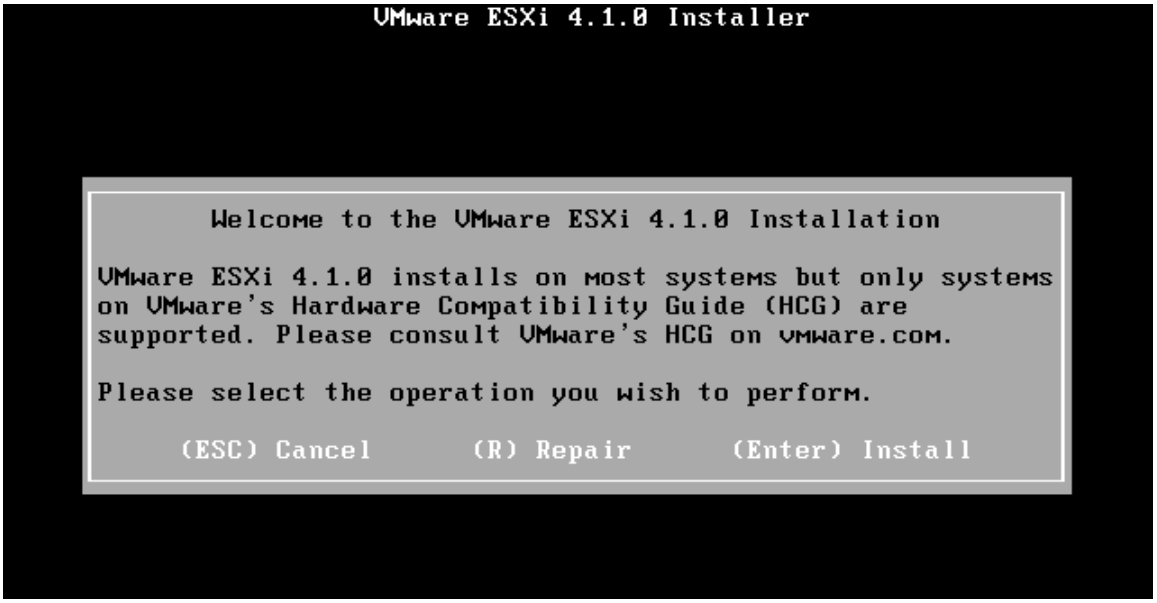
After downloading the ISO image, burn it to CD. The recorded disk will enable you to install the VMware ESXi system on a dedicated server.

2.4 Installation of VMware ESXi operating system

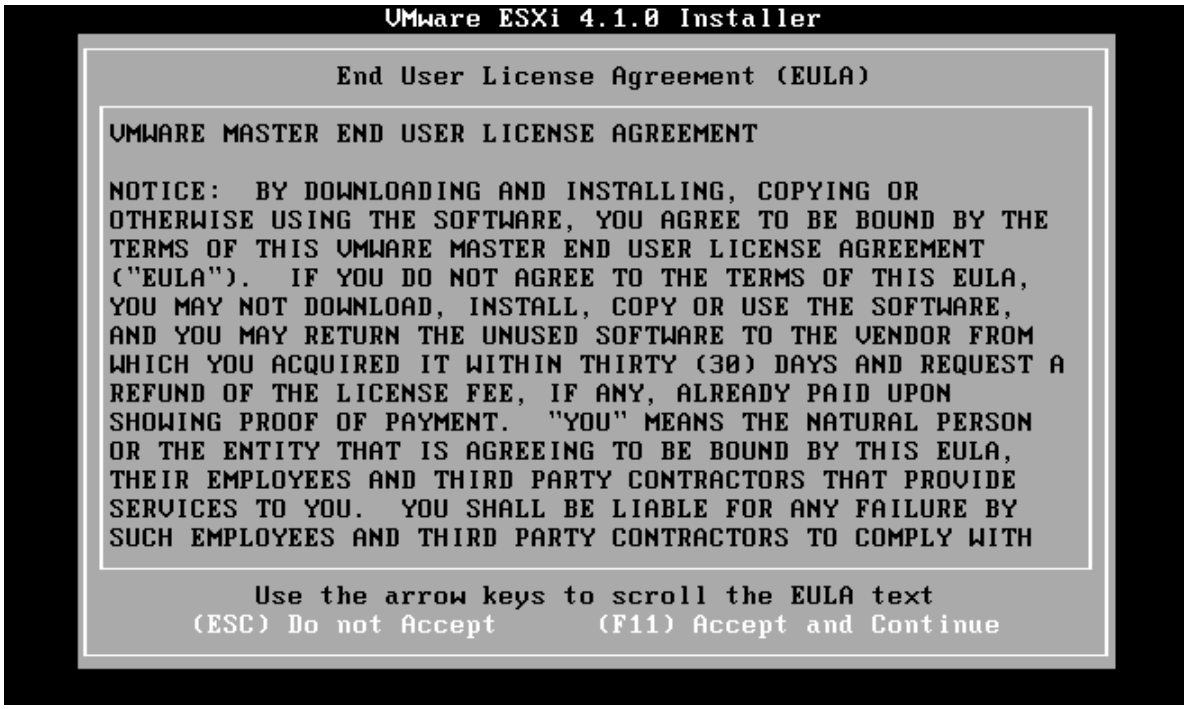
1. Turn on the server and insert the recorded CD into the drive.
2. Select the ESXi Installer option and confirm by pressing ENTER.



3. A message will be displayed to inform you that the system may only be installed on the hardware which meets the requirements listed earlier in this manual. Press ENTER to continue the installation.

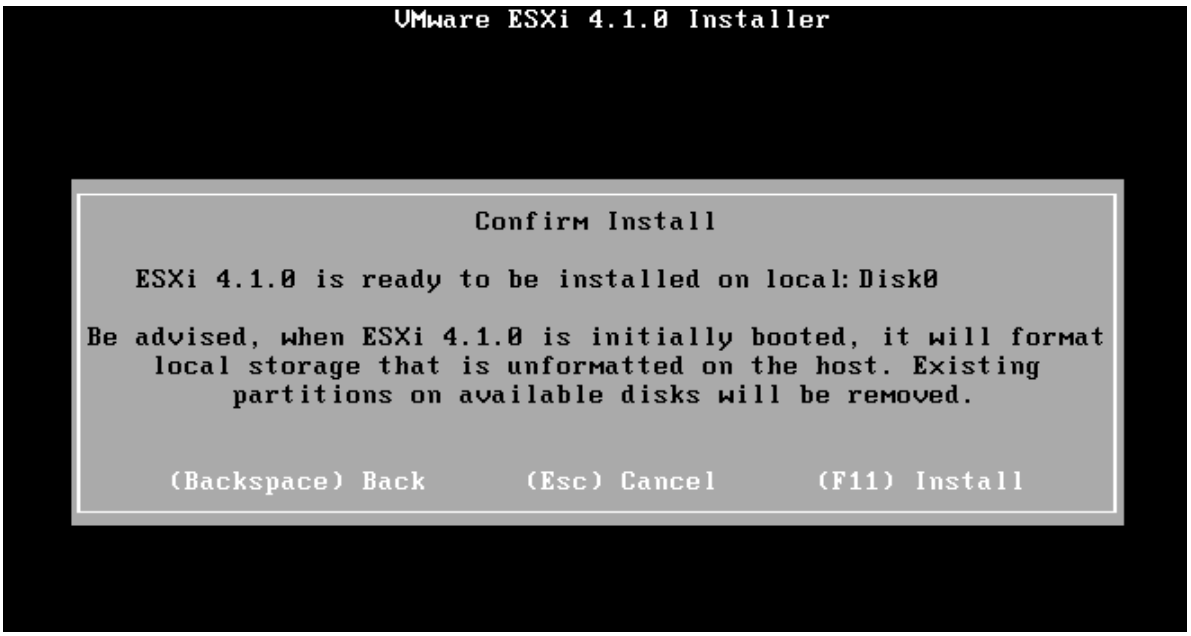


4. After reading the license terms, press F11 to accept them.

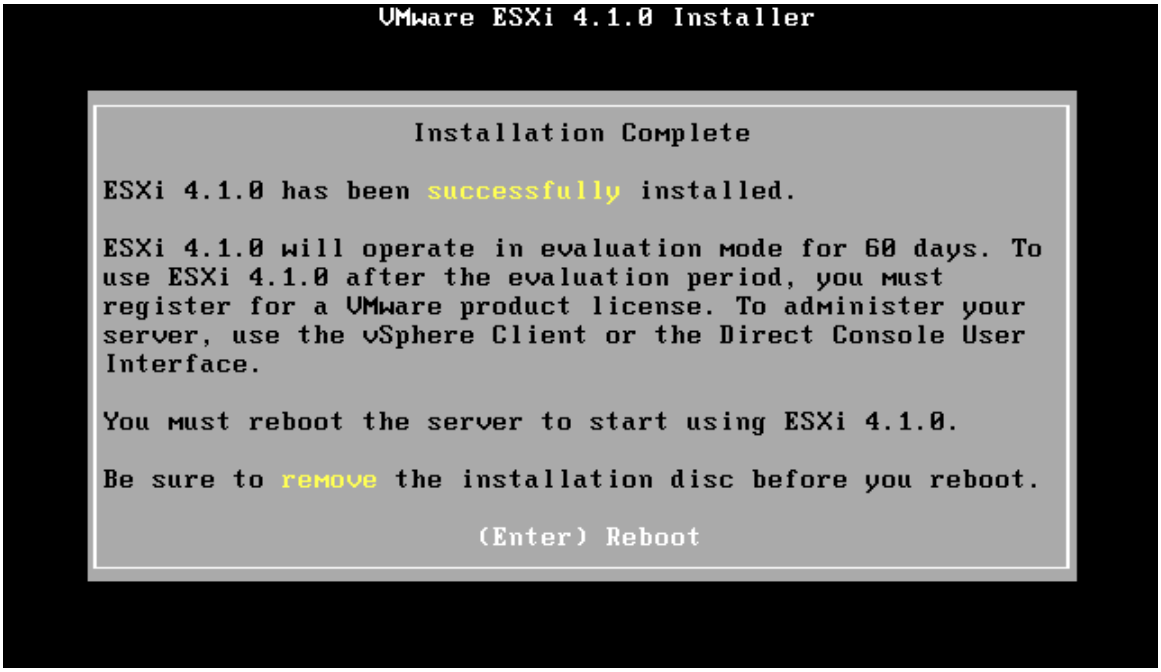


5. A list of drives available on the server will be displayed. Select that on which you want to install the operating system and confirm by pressing ENTER.

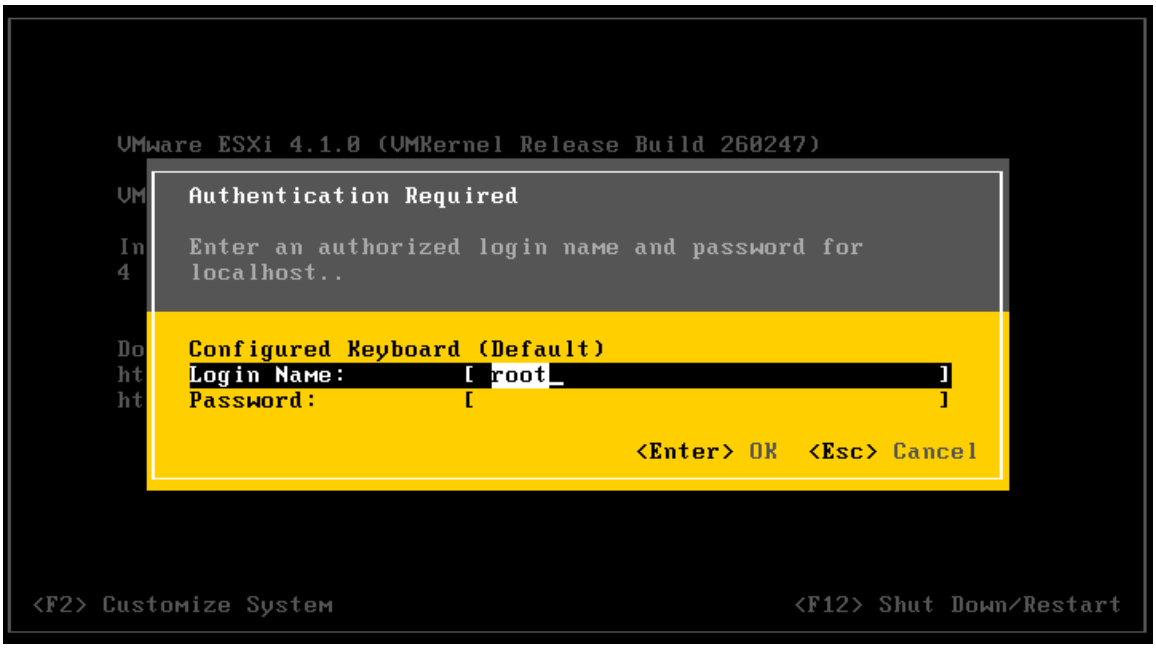
6. Press F11 to start the next installation steps.



7. Having completed the installation, remove the CD from the drive, and then press ENTER to restart your computer.

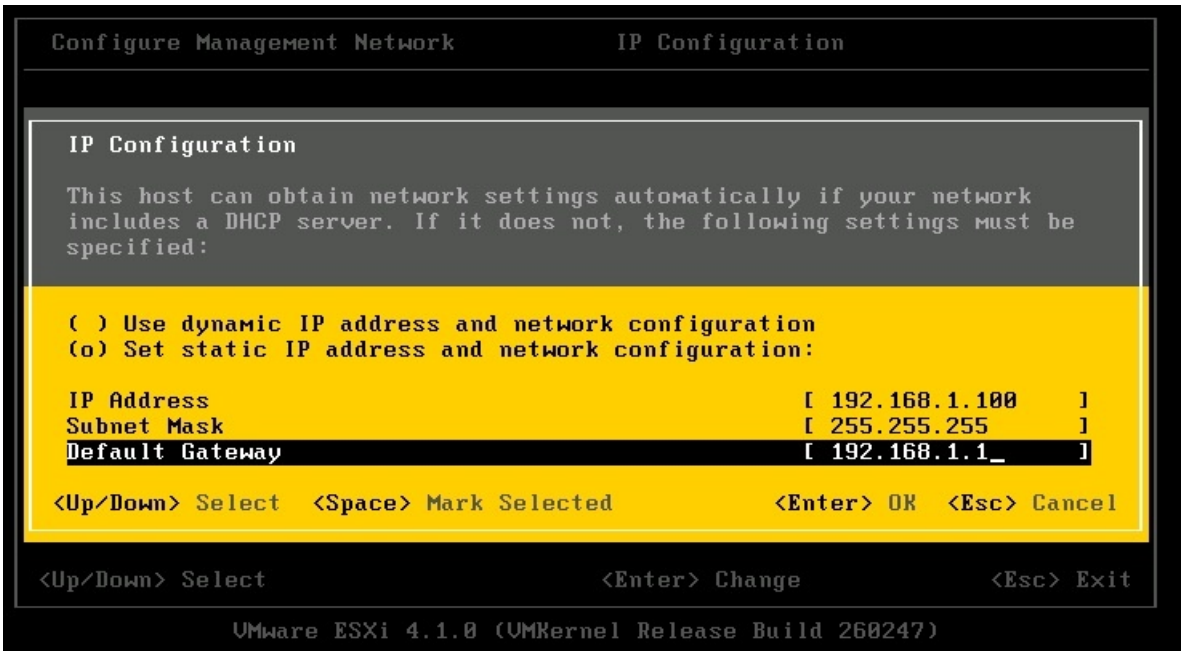


8. After installing the VMware ESXi operating system and rebooting the computer, the "Authentication Required" window will be displayed. Press ENTER to accept the already entered data and go to the next window.

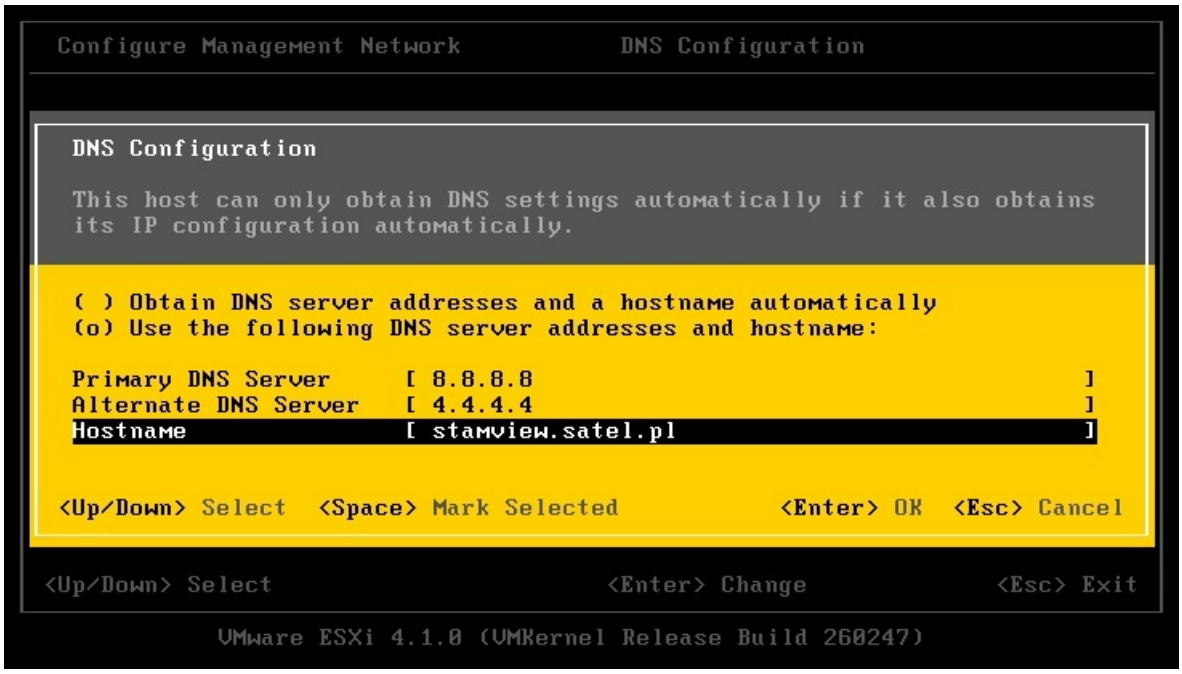


9. Press F2 to go to the basic configuration of the server and its network settings. Choose "Configure Password" and define a password for the server. The password can contain from 8 to 40 characters (letters and digits). Confirm your changes by pressing ENTER. Press ESC to go back to the server settings main menu.

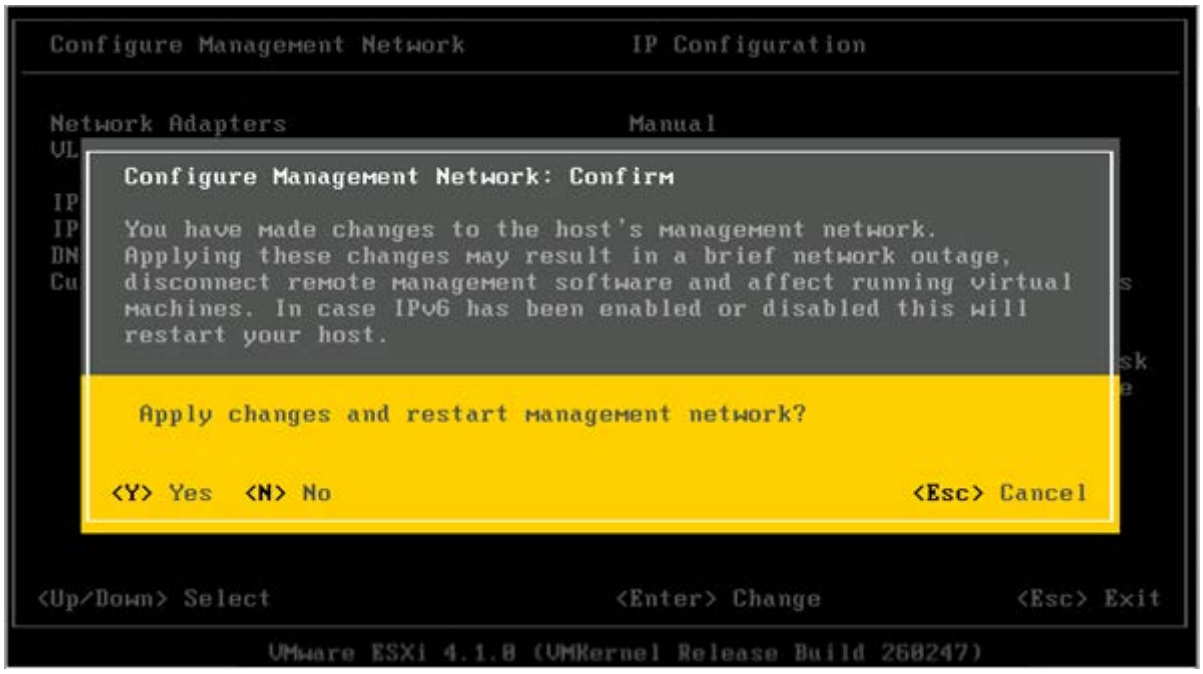
10. Select the "Configure Management Network" command, and the "IP Configuration" in it. If the network address is assigned dynamically by the server to the DHCP server, leave the "Use dynamic IP address and network configuration" option selected. If the server's network address is to be entered manually, select the "Set static IP address and network configuration" option and enter the appropriate data in the "IP Address", "Subnet Mask" and "Default Gateway" fields. Press ENTER to confirm your changes. Then press ESC to return to the server settings main menu. The data below are given for example purpose only.



11. If the network settings have been entered manually, you must also configure the DNS server address. Select the "DNS Configuration" command and enter the DNS server IP addresses into the "Primary DNS Server" and "Alternate DNS Server" fields, and the VMware ESXi server name into the "Hostname" field. Press ENTER to confirm your changes. Press ESC to return to the server settings main menu. The data below are given just as a sample.



12. Having entered the network data, press ESC to exit the menu, and then press "Y" to confirm the new settings.



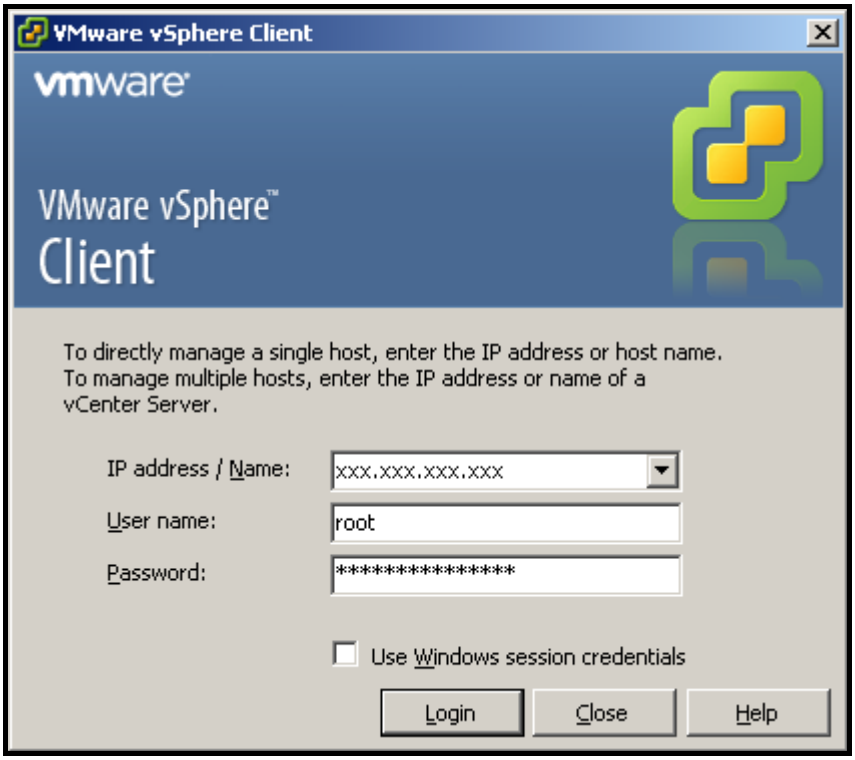
2.5 Installation of VMware vSphere Client program

1. Open the web browser window and enter the IP address of VMware ESXi server. Once connected, click on the "Download vSphere Client" link to start installation of the program.
2. After the installation is complete, run the program by clicking on the program shortcut created on the desktop or in the Start menu.
3. Data to be given during login:

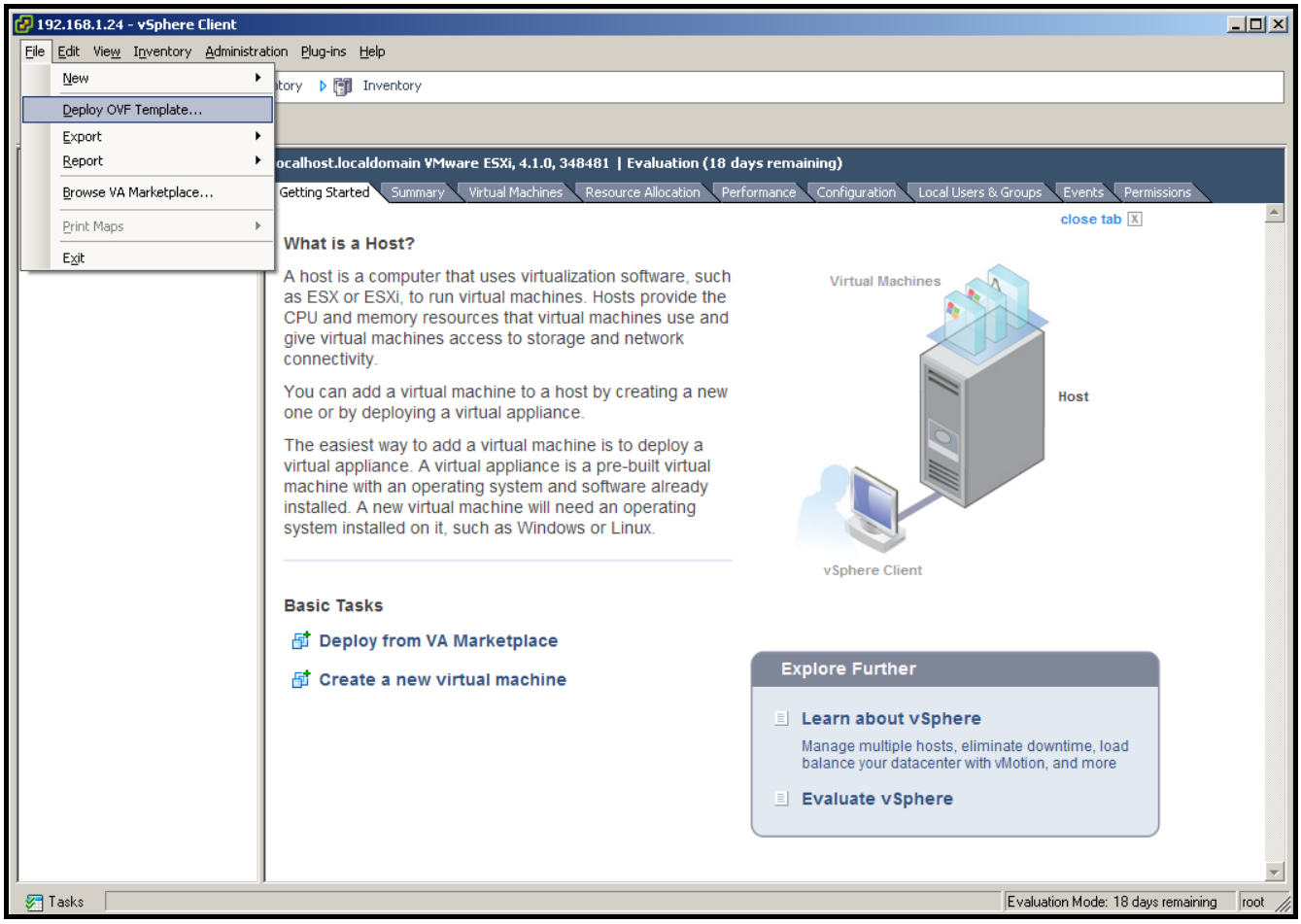
   IP address / Name: enter the IP address or name of the server where the VMware ESXi system is installed,

   User name: enter "root",

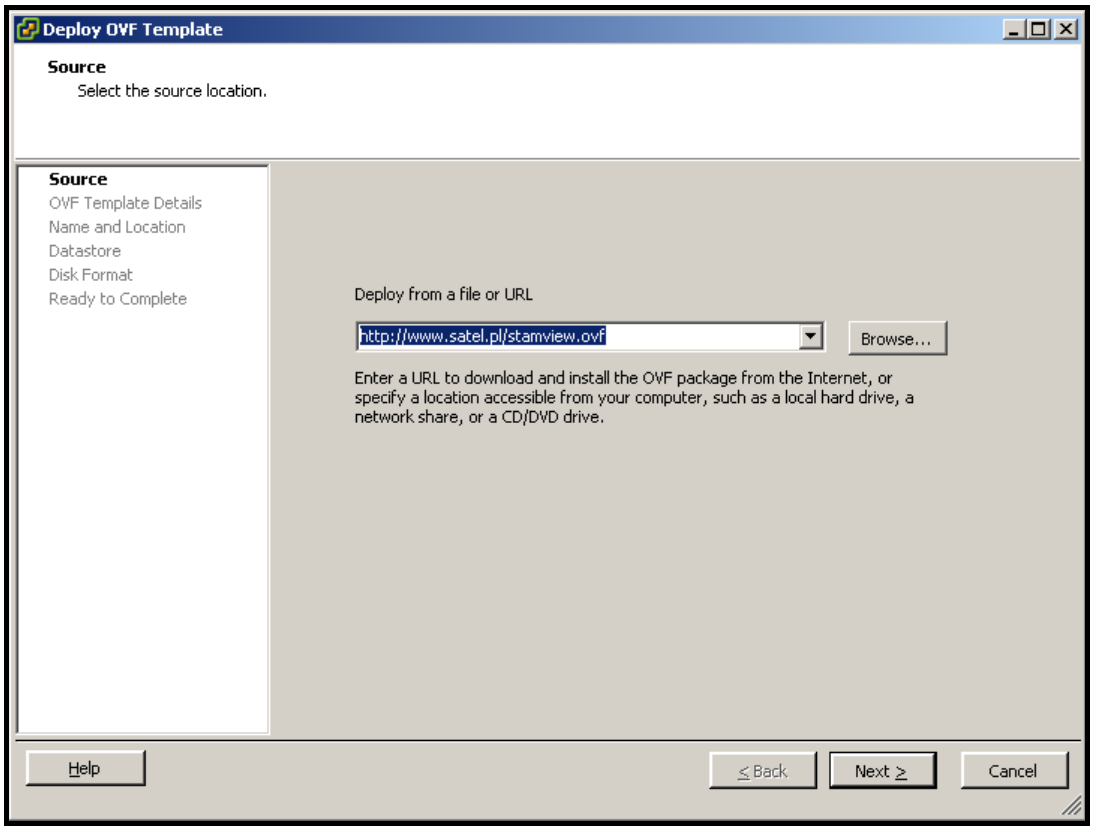
   Password: enter the password you gave during configuration of the VMware ESXi.



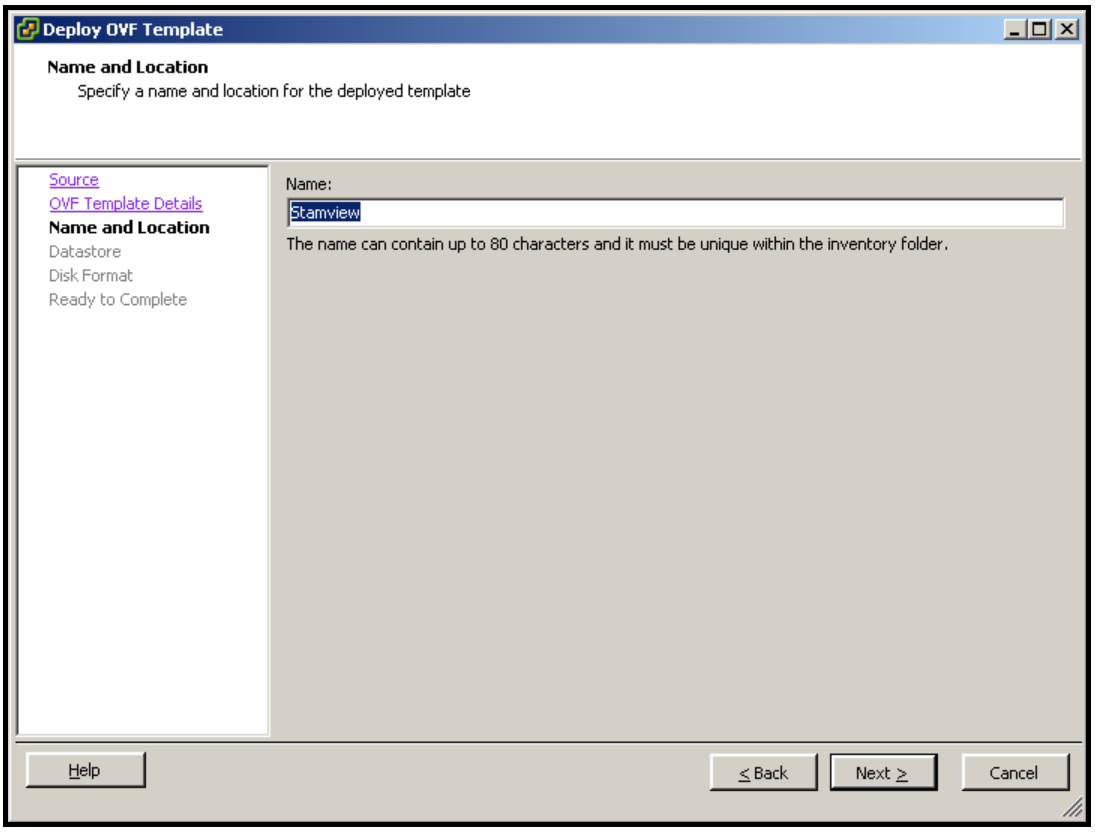
4. Select the "Deploy OVF Template" command in the "File" menu.



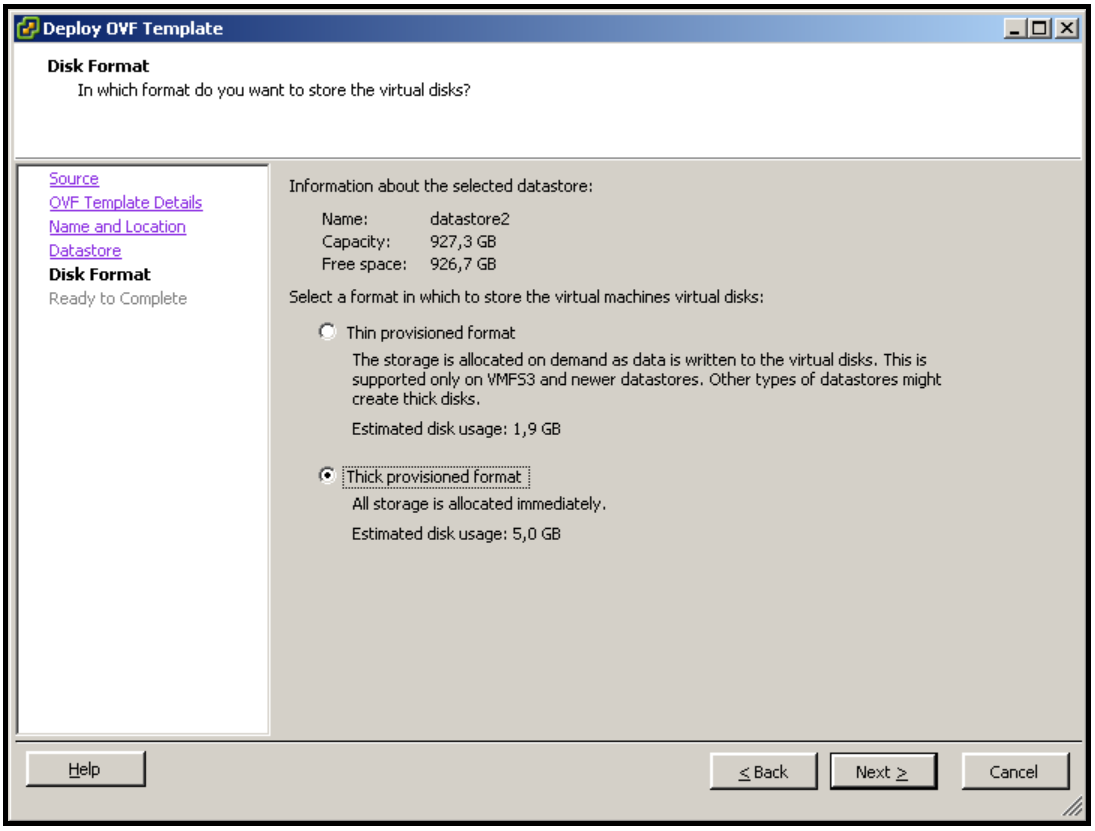
5. Enter the http://www.satel.pl/stamview.ovf address in the "Deploy from a file or URL" field and press NEXT.



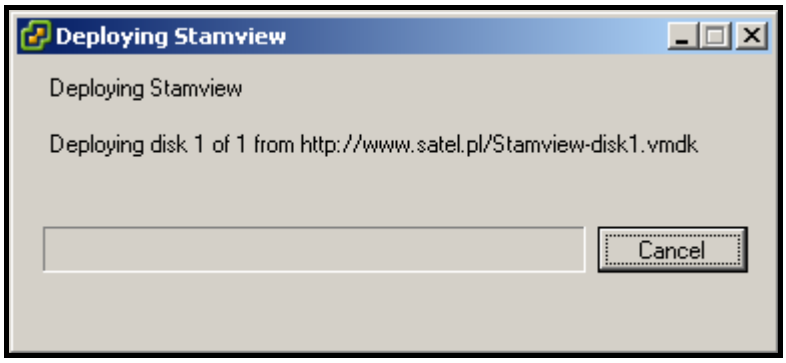
6. Enter the name of STAM-VIEW virtual machine and press NEXT.



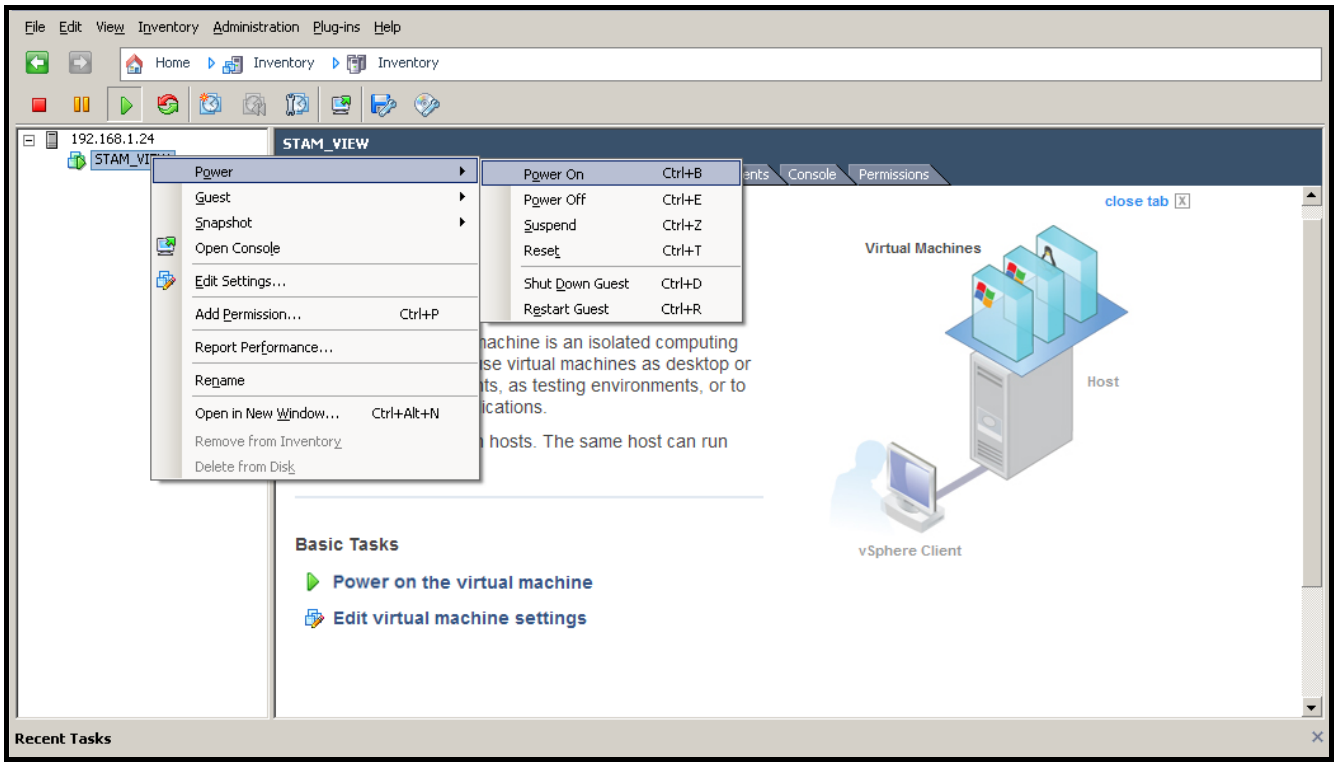
7. Select the disk on which the virtual machine is to be deployed and press NEXT.
8. Select the "Thick provisioned format" option and press NEXT.



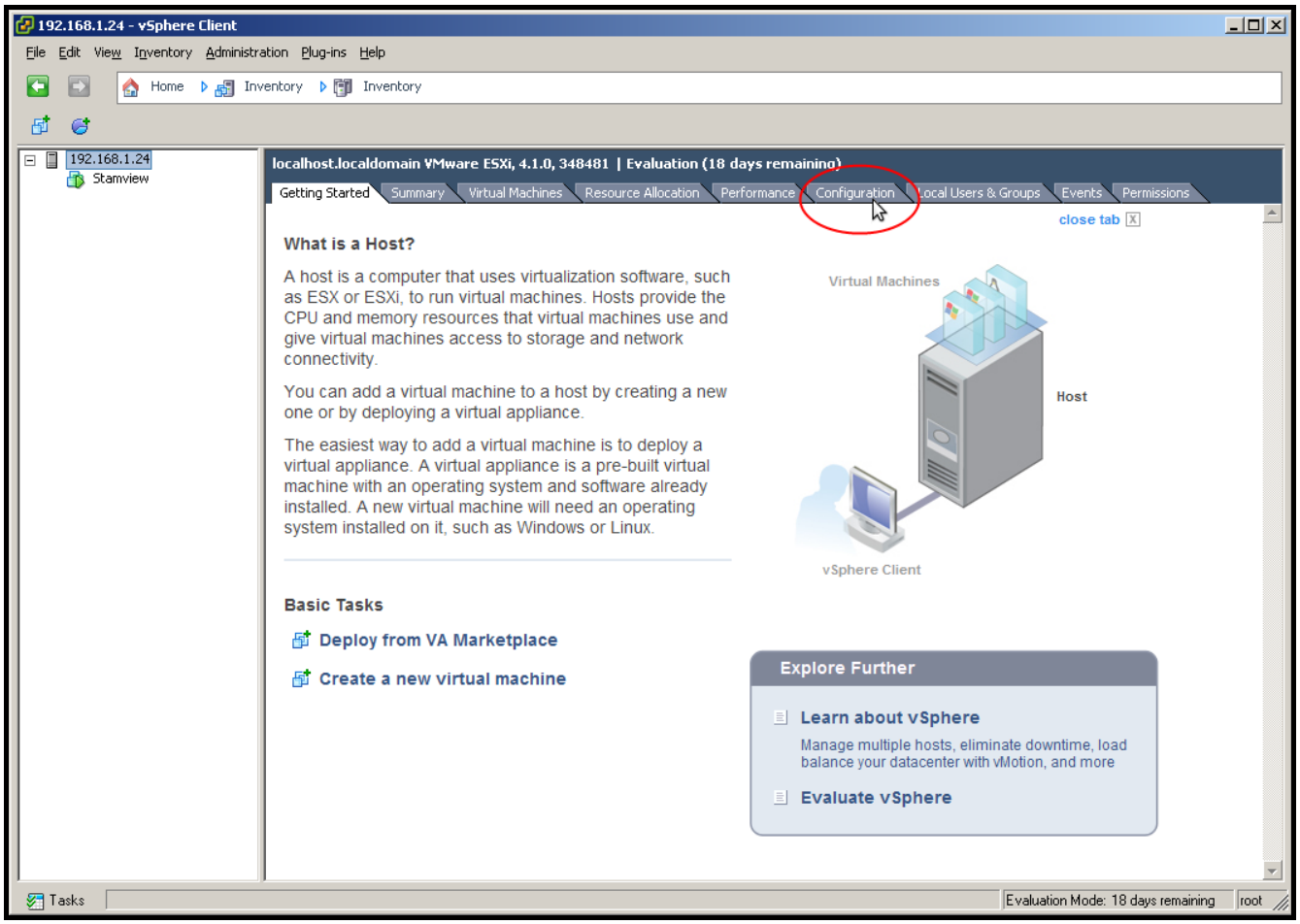
9. A summary of data on the virtual machine settings will be displayed. Press FINISH. The STAM-VIEW environment takes more than 530 MB, so the process of its importing may last up to about 1 hour.



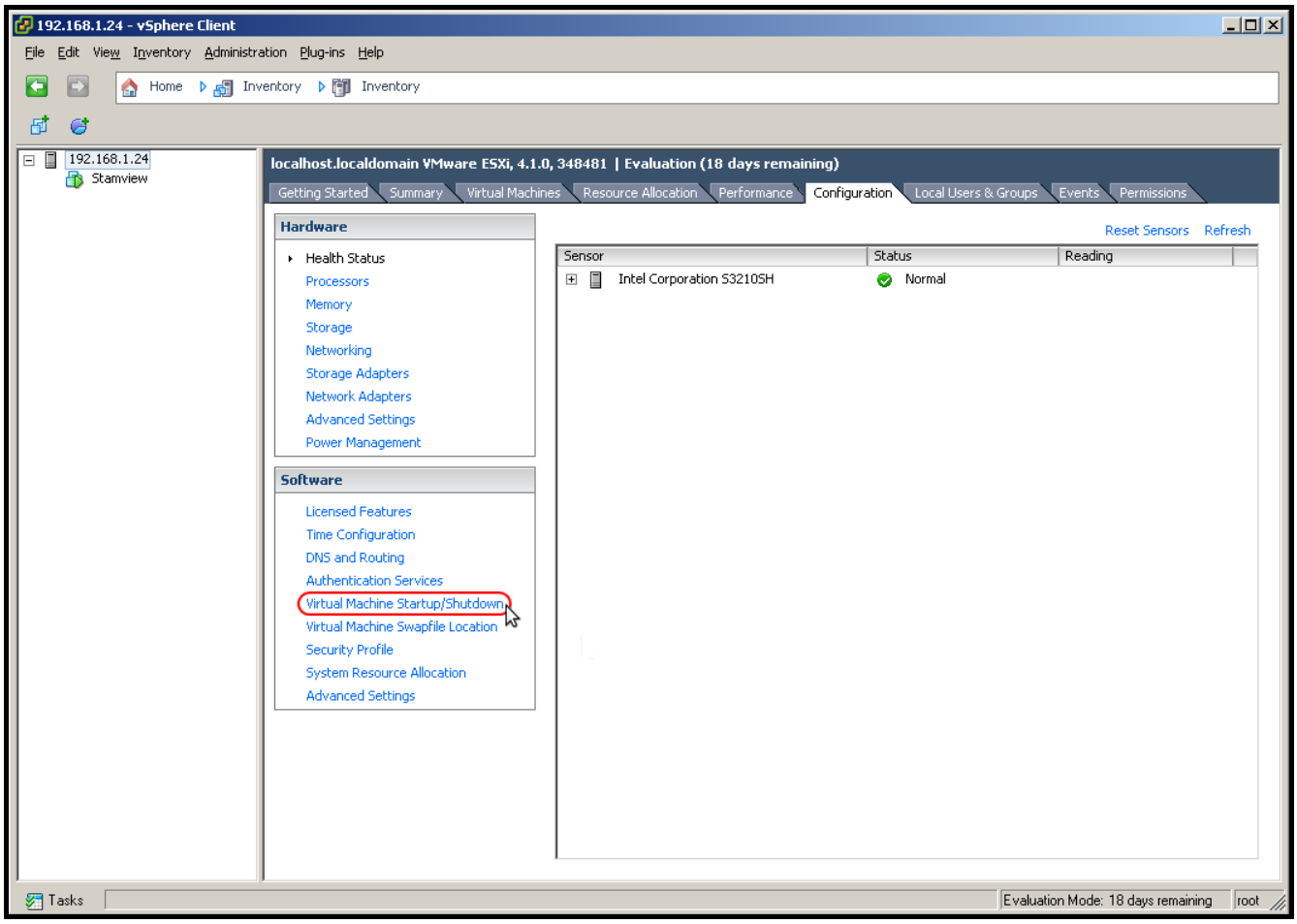
10. In order to run the imported machine, set the mouse cursor over the machine name and right-click. In the drop-down menu, click "Power" and then "Power On". The IP address of the machine with STAM-VIEW system installed, as shown in the screenshot, is just an example.



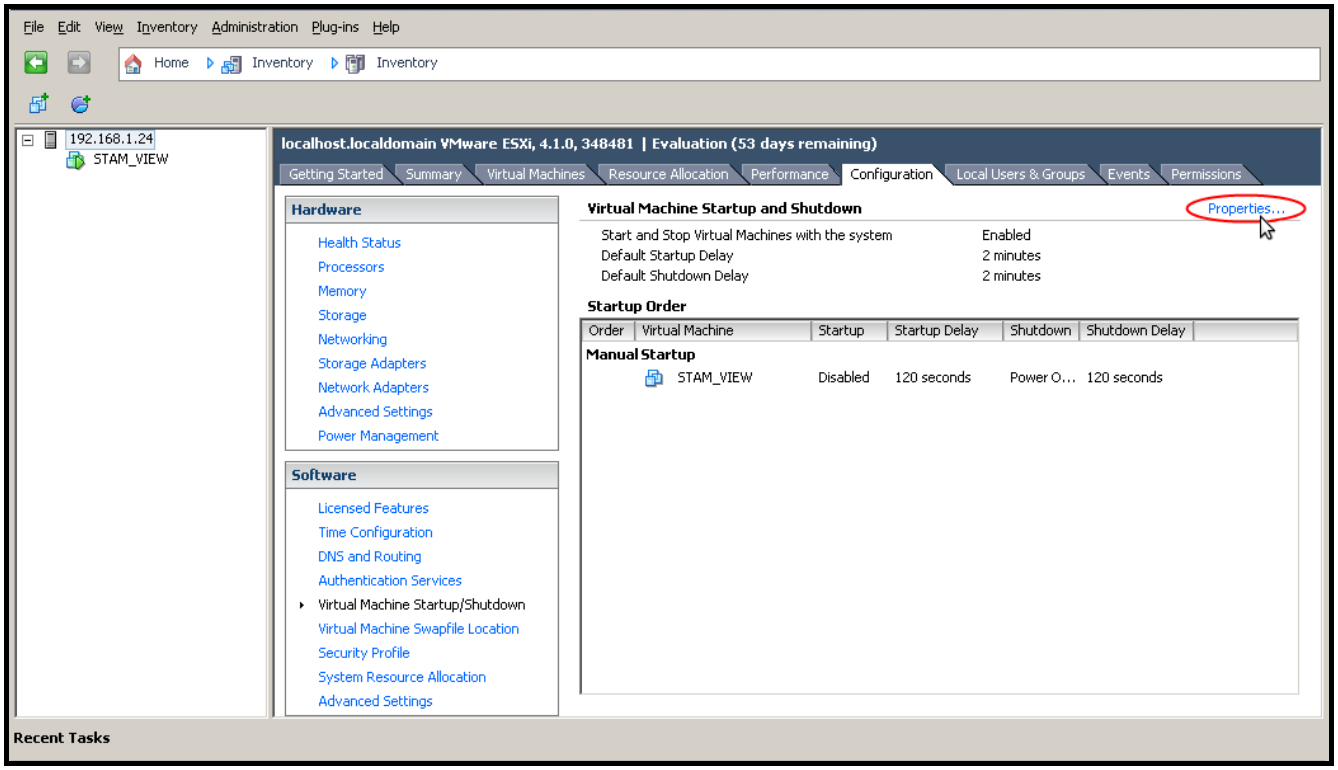
11. Turn the machine to run automatically. To do so, hover your mouse cursor over the machine address and left-click. You will see tabs with the server-related data. Select the "Configuration" tab.



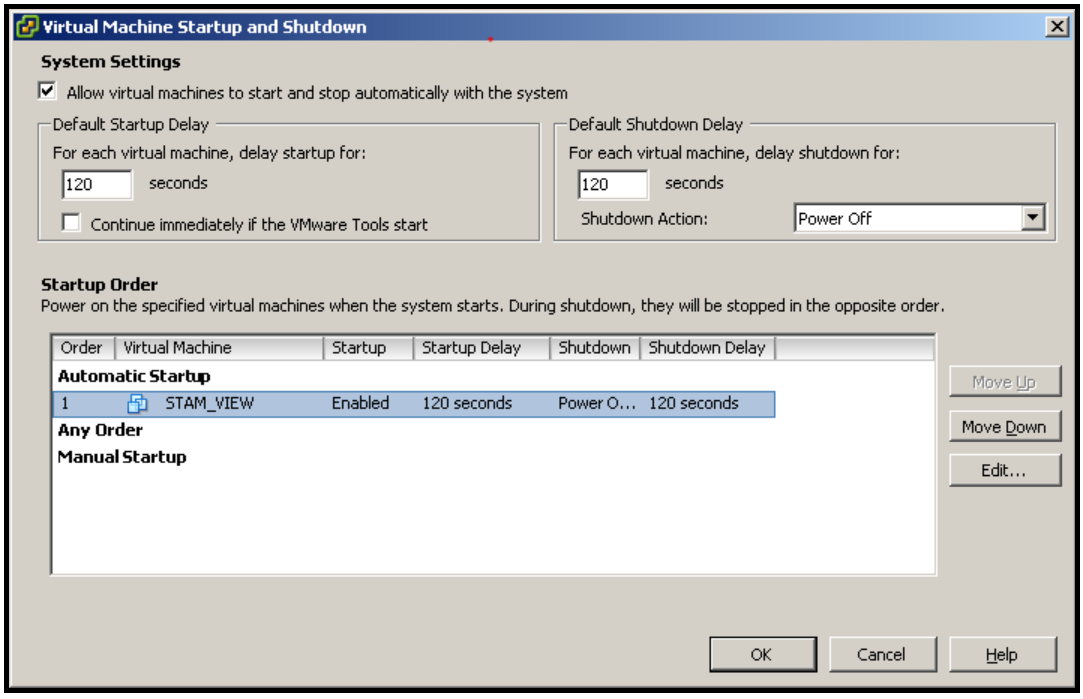
12. Click on "Virtual Machine Startup / Shutdown" in the "Software" area.



13. Select "Properties" in the upper right corner of the window.



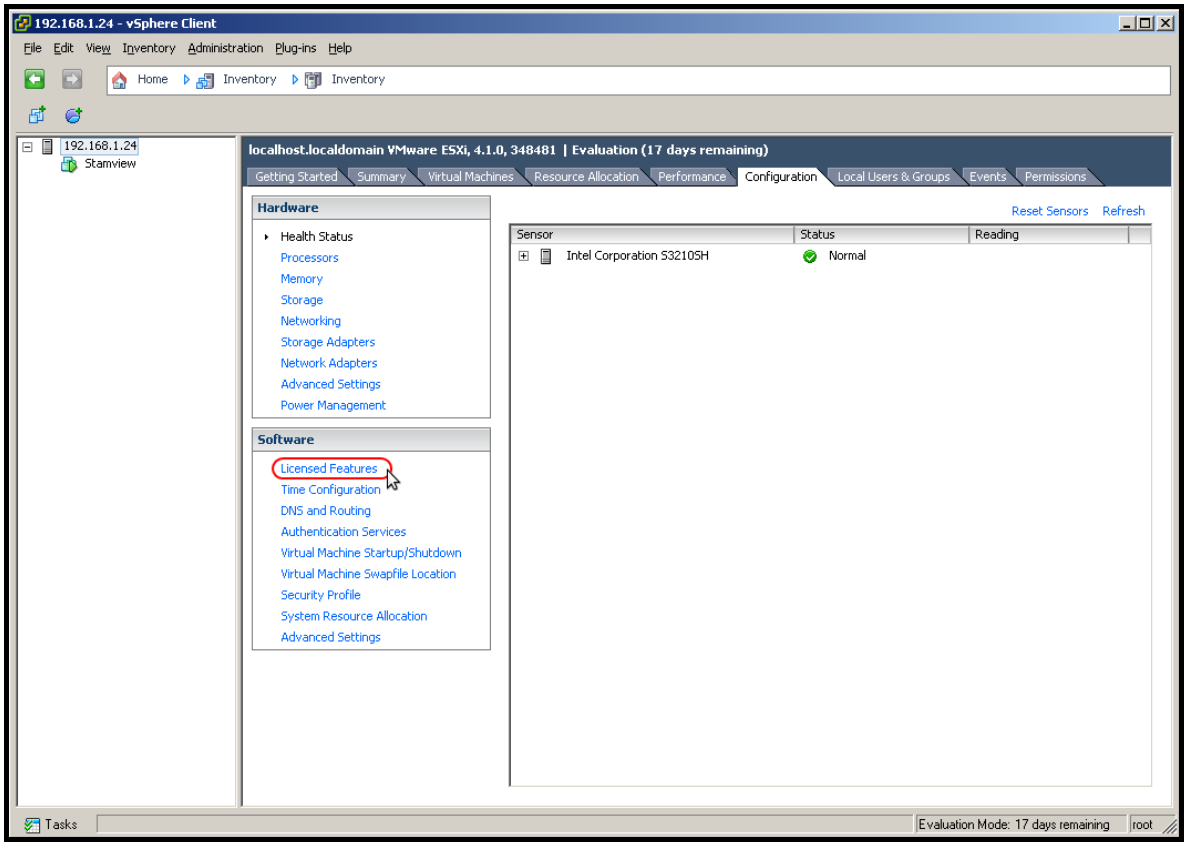
14. Select the "Allow virtual machines to start and stop automatically with the system" option. Then select the "STAMVIEW" virtual machine and using the "Move Up" button move it to the "Automatic Startup" area.



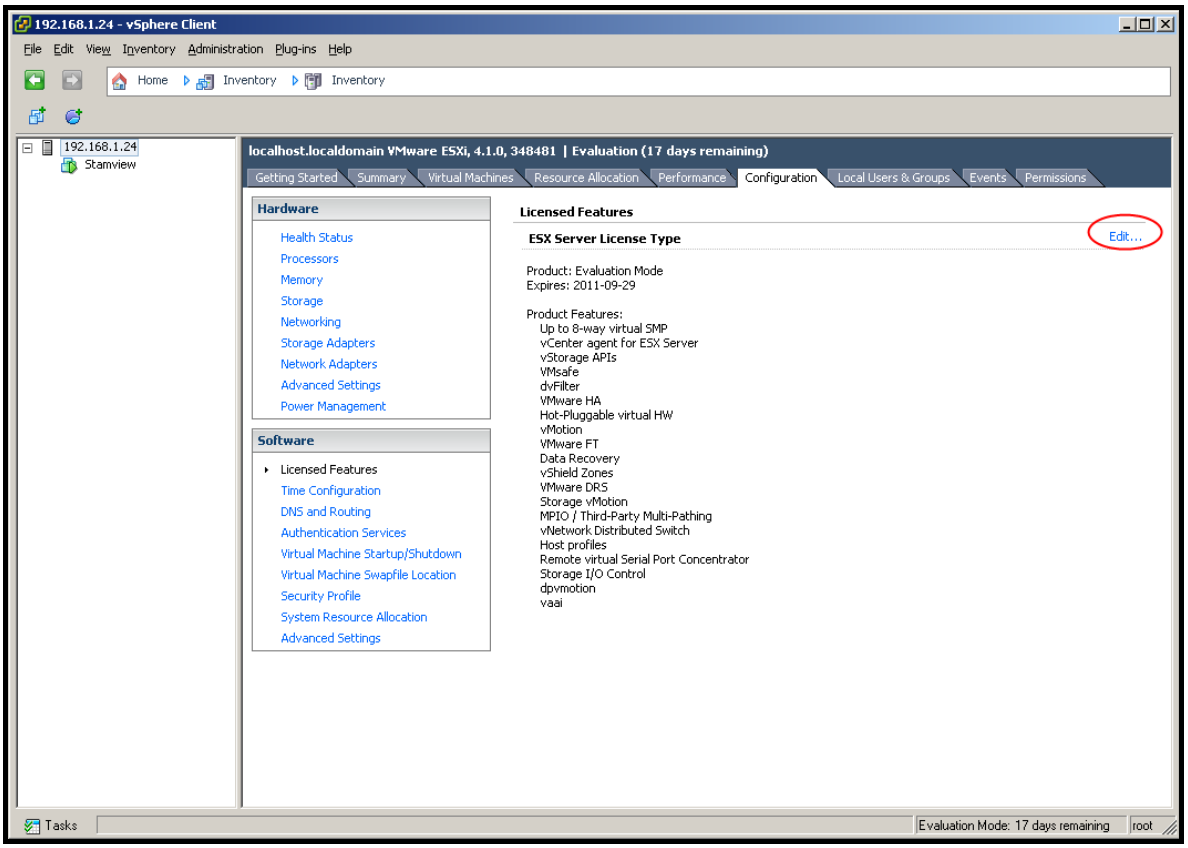
2.5.1 Entering license key

Be sure to enter the license key which is required for the proper operation of the program beyond the 60-day period. The key is available after you log in to your account on the site of the VMware software manufacturer.

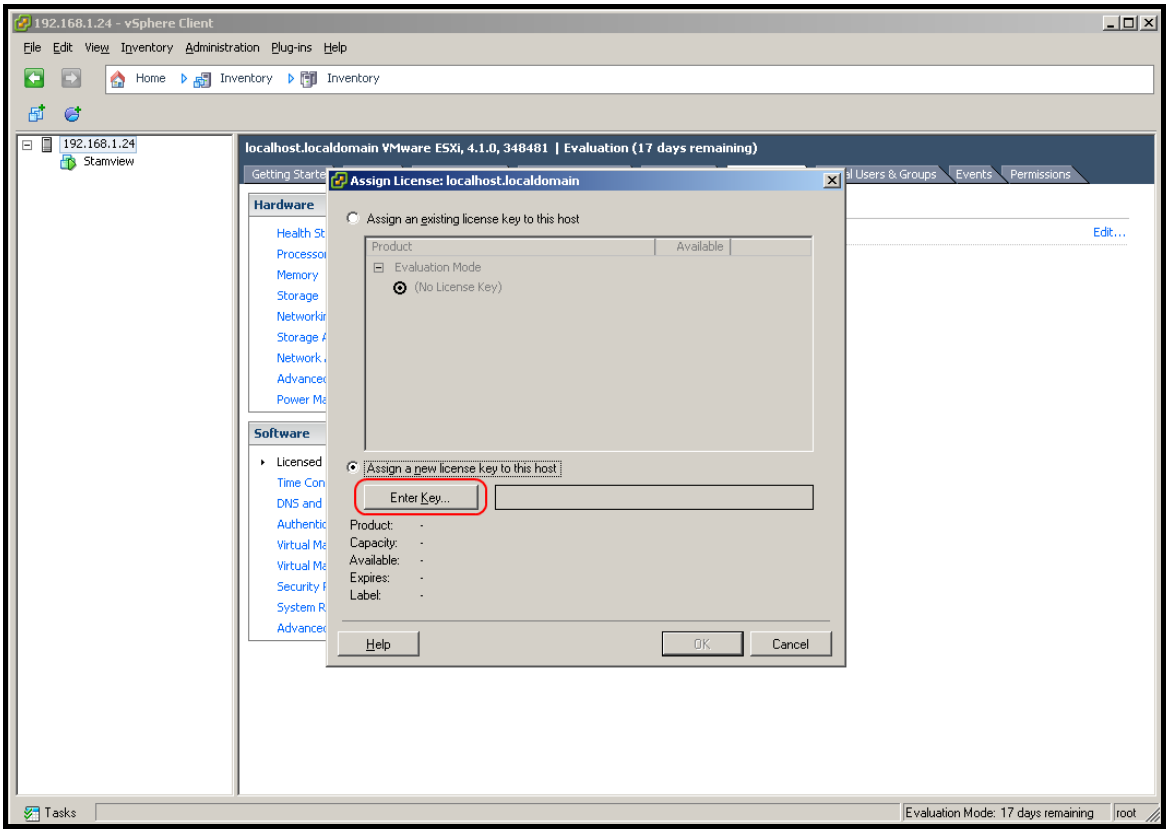
1. In the "Configuration" tab, click on the "Licensed Features" in the "Software" area.



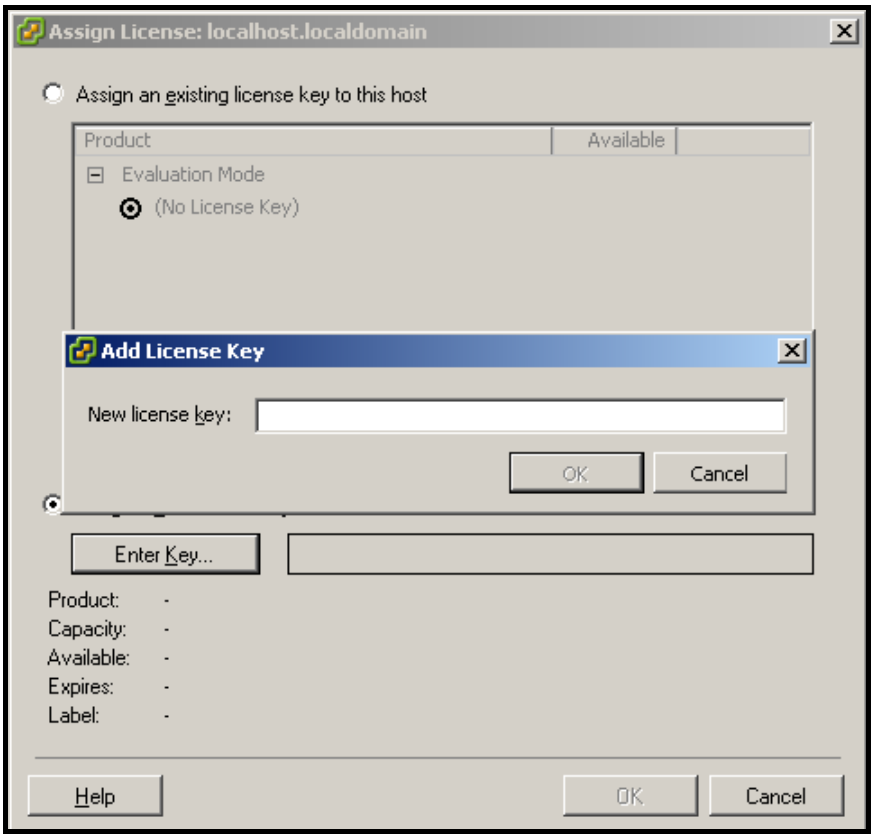
2. Select "Edit" in the upper right corner of the window.



3. Select the "Assign a new license key to this host" command. Press "Enter Key ...".



4. In the "Add License Key" window, enter the code in the "New license key" field. Click "OK".



5. Click "OK" in the "Assign License" window.

3. SSL certificates

Generating appropriate SSL certificates is required to confirm the security of Internet browser connection to the server. After the first login to STAM-VIEW system, the "Default (change required)" message will be displayed for the SSL certificates and the "StartSSL" message for the authorizing body certificates at their status. Therefore, the suitable certificate and key must be generated, and then downloaded to the STAM-VIEW system.

Notes:

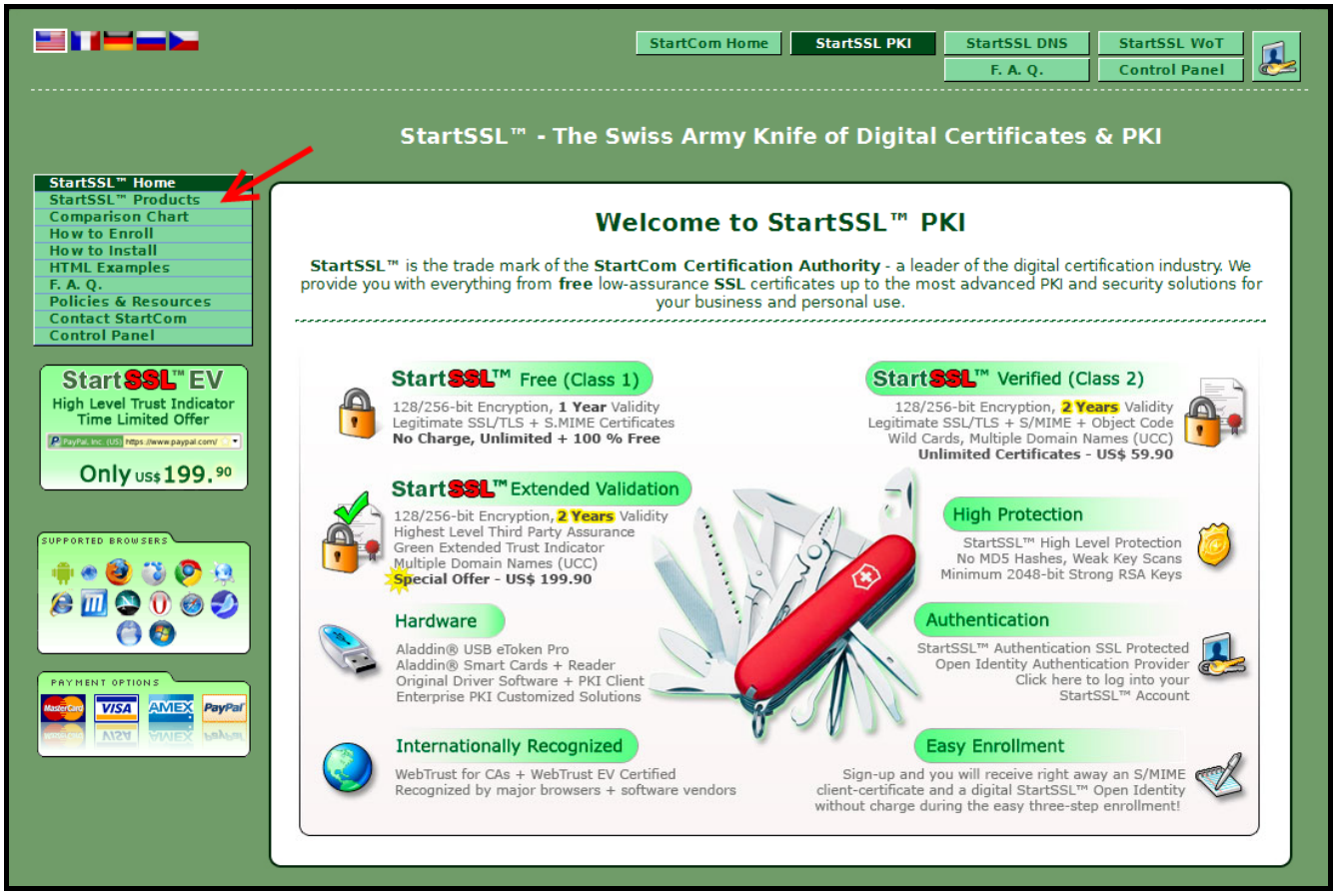
- *You can only obtain a free SSL certificate when you are the domain owner.*
- *The SSL certificates will only work correctly if the VMware ESXi server address is specified in the form of a domain name during installation.*

3.1 StartCom certificates (recommended)

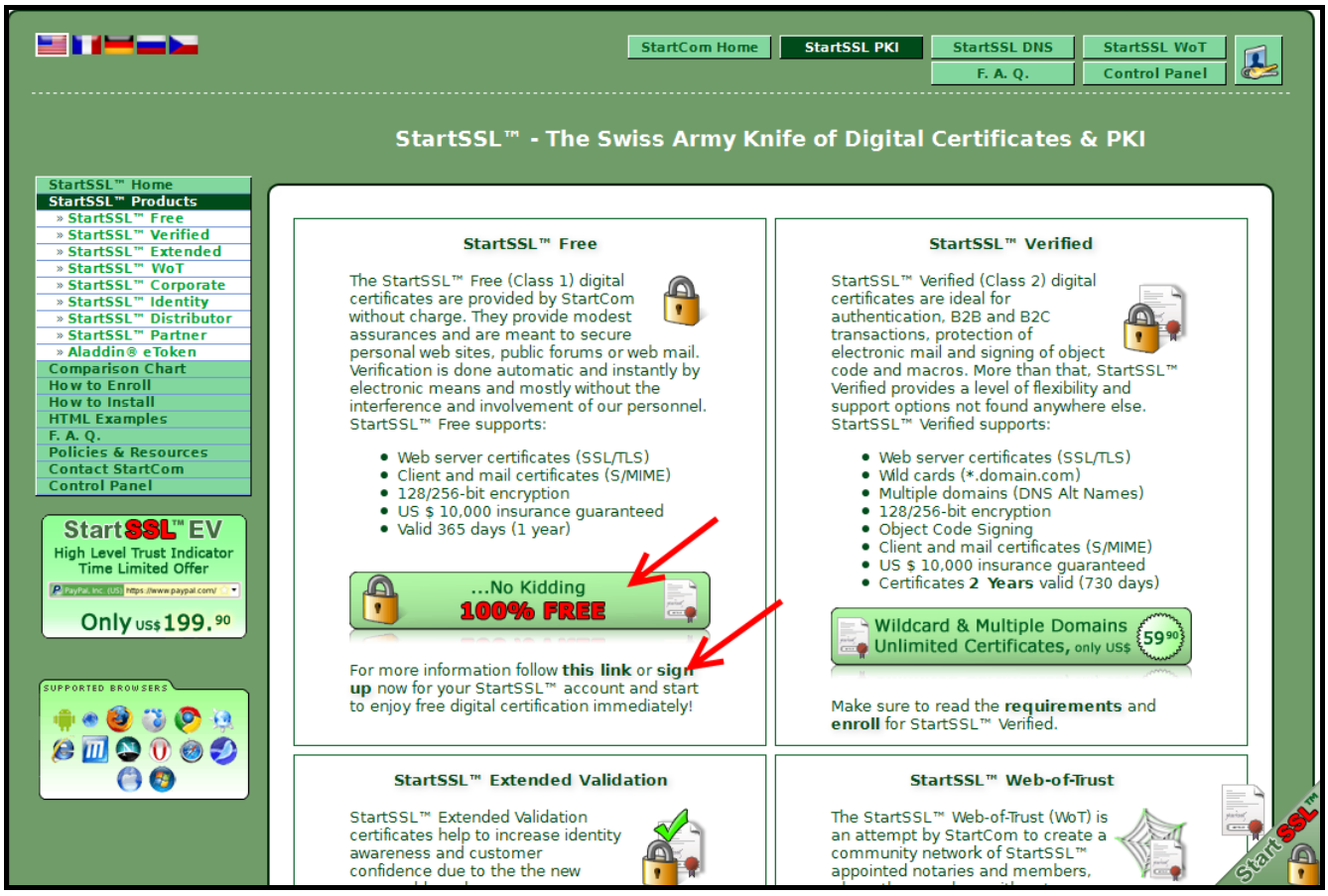
In order to generate the certificate and key, the administrator must perform the following steps:

1. Type in the www.startssl.com address in your web browser.

2. Select the "StartSSL ™ Products" tab in the upper left portion of the window.

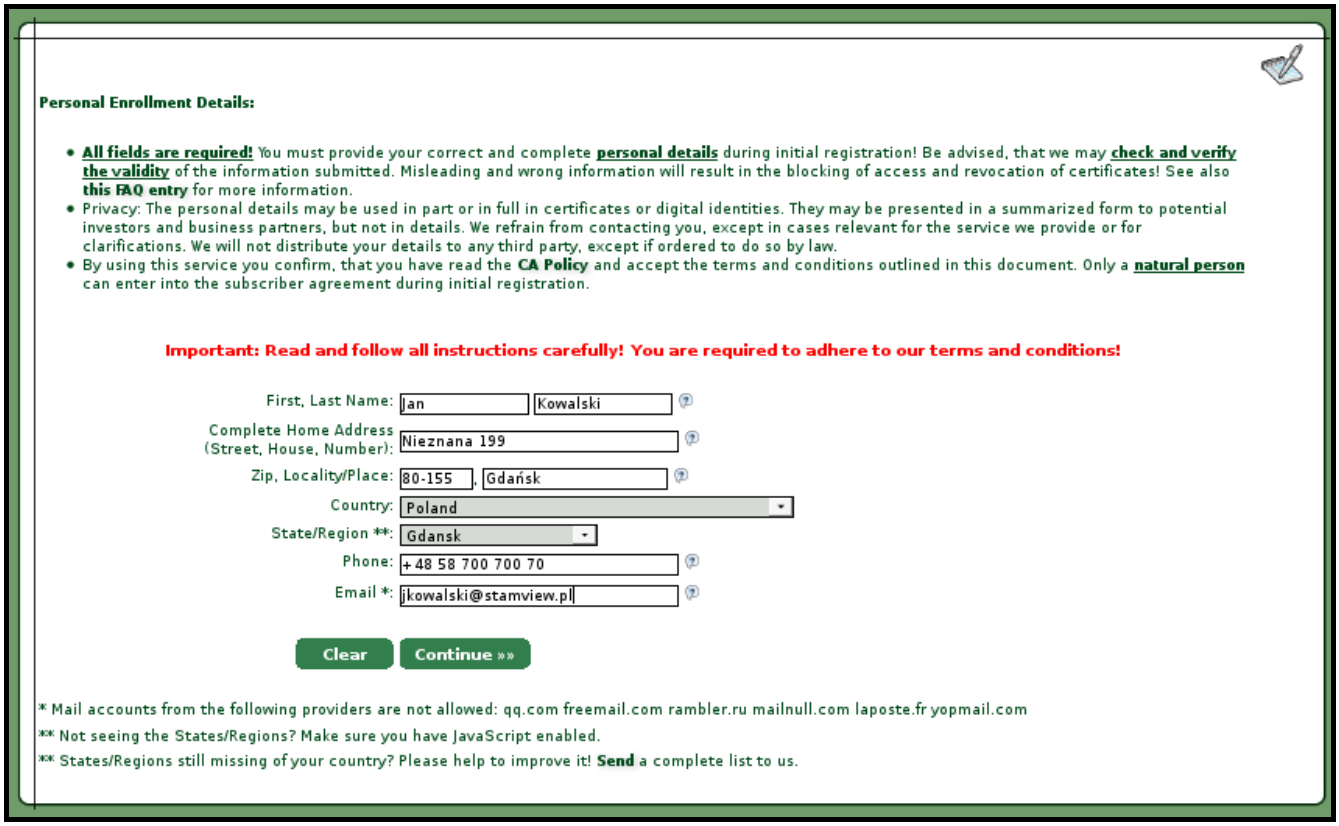


3. Click on the green panel with the lock icon or on the "sign up" link in the "StartSSL ™ Free" section.



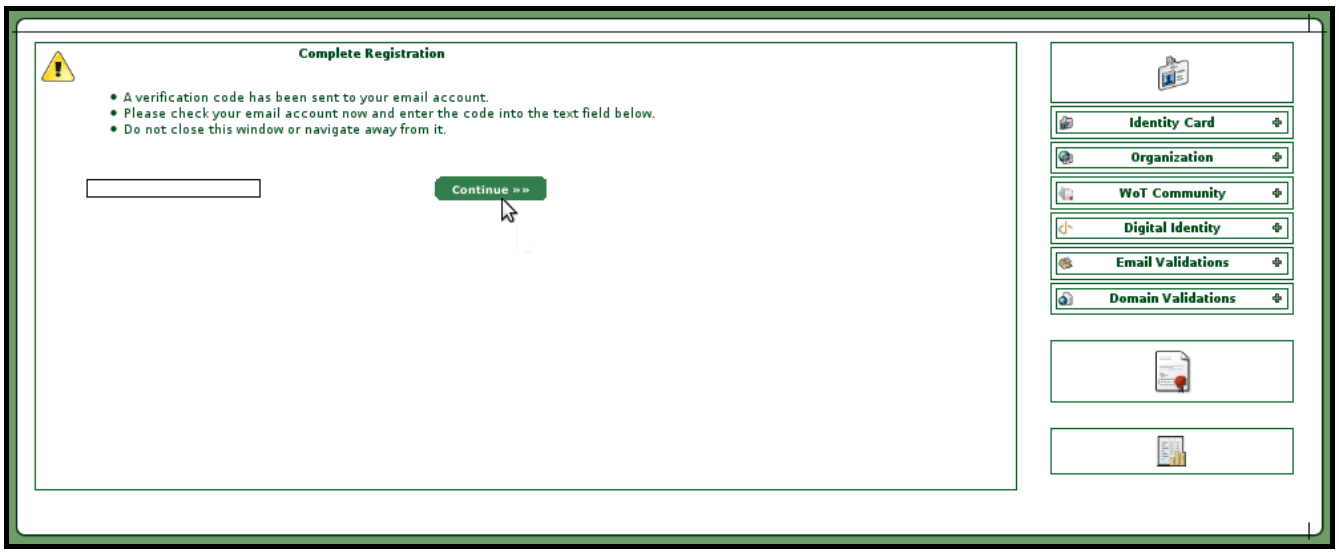
4. A window will open. Select "Sign-up".

5. Read carefully the instructions on the page, fill in all the fields necessary for the registration and click the "Continue" button.



Note: *During registration, the administrator must provide some private personal data, otherwise not being authorized to generate a free certificate and key.*

6. A window will open. Click "OK".
7. Check the mailbox whose address was specified during registration. The received e-mail message should contain the user verification code that should be entered in the empty field. Click the "Continue" button.

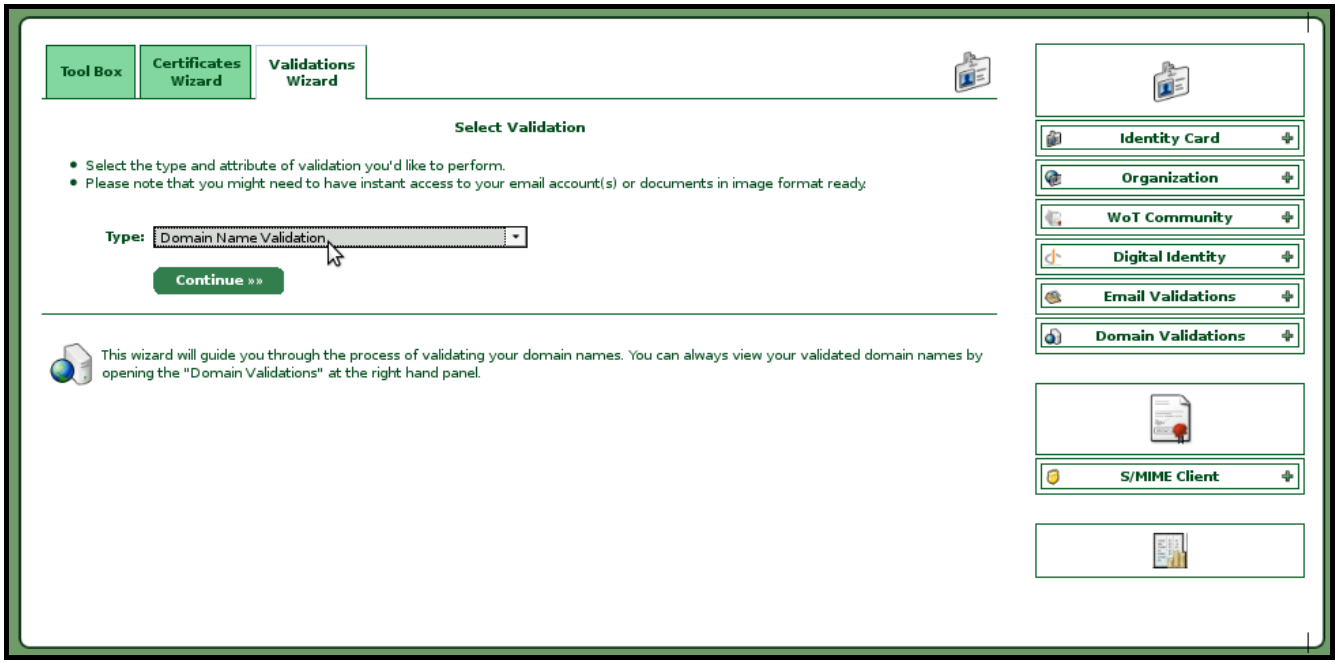


8. Click the "Continue" button in the window with information on generating a private key for the user's personal certificate, which is required to properly communicate with the www.startssl.com page.
9. Click the "Install" button to install the personal certificate.

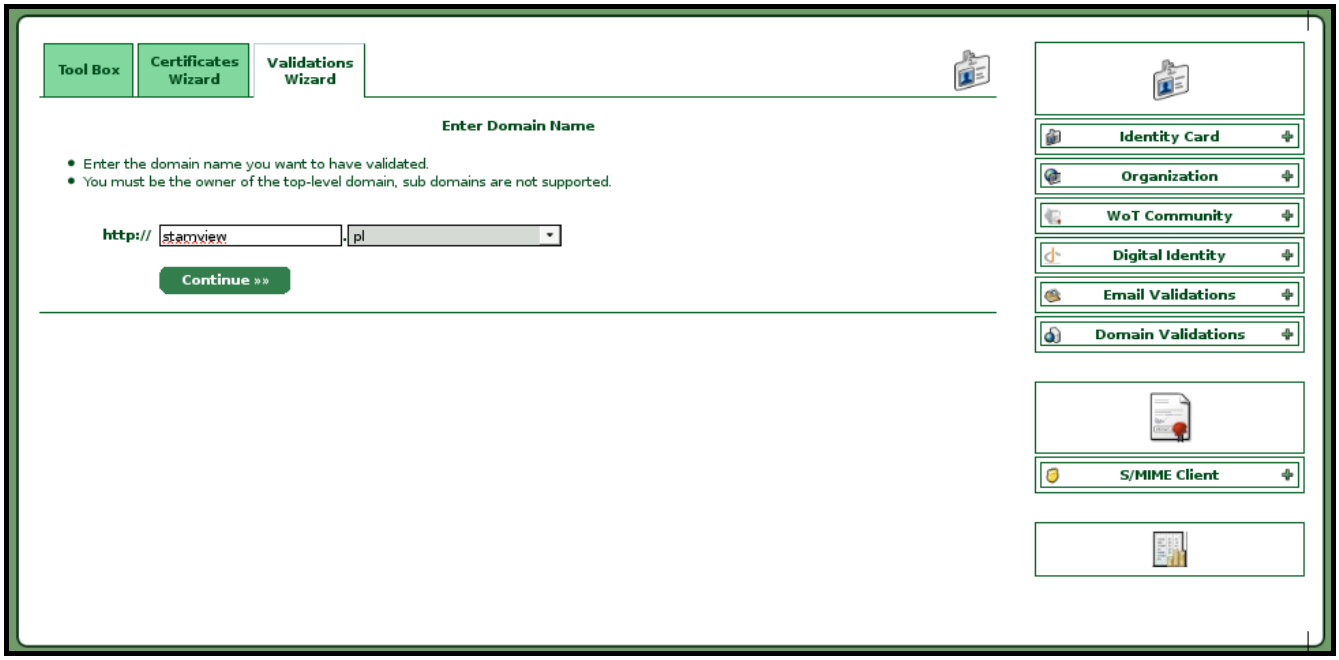
10. The certificate will be permanently installed in your web browser. It is recommended that you keep a backup copy of it (to do so, see the "How do I backup my client certificates?" instructions in the "F. A. Q." tab at the http://www.startssl.com/?app=25 web page). Click "Finish".

11. A tabbed window will open. The tabs will make it possible to carry out verification of the domain owner and to generate the ssl.crt certificate and the ssl.key code. Select the "Validations Wizard" tab.

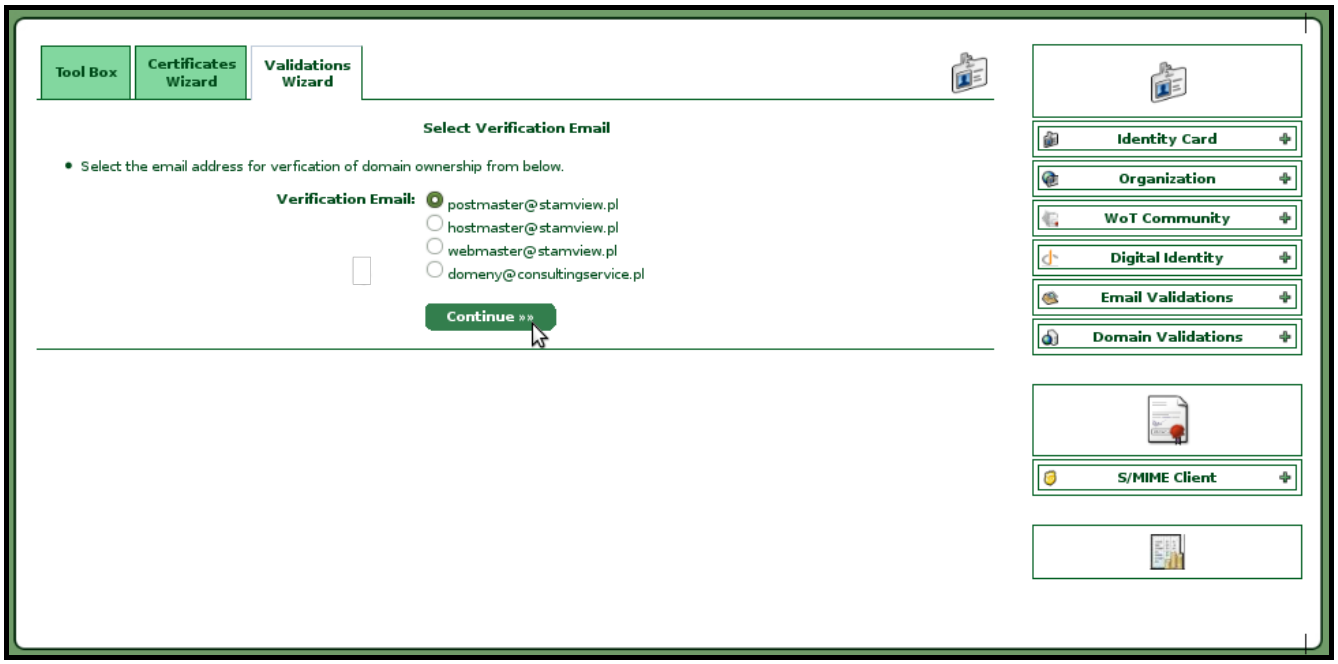
12. In order to validate the domain owner, select the "Domain Name Validation" in the "Type" field of the dropdown menu, and click "Continue".



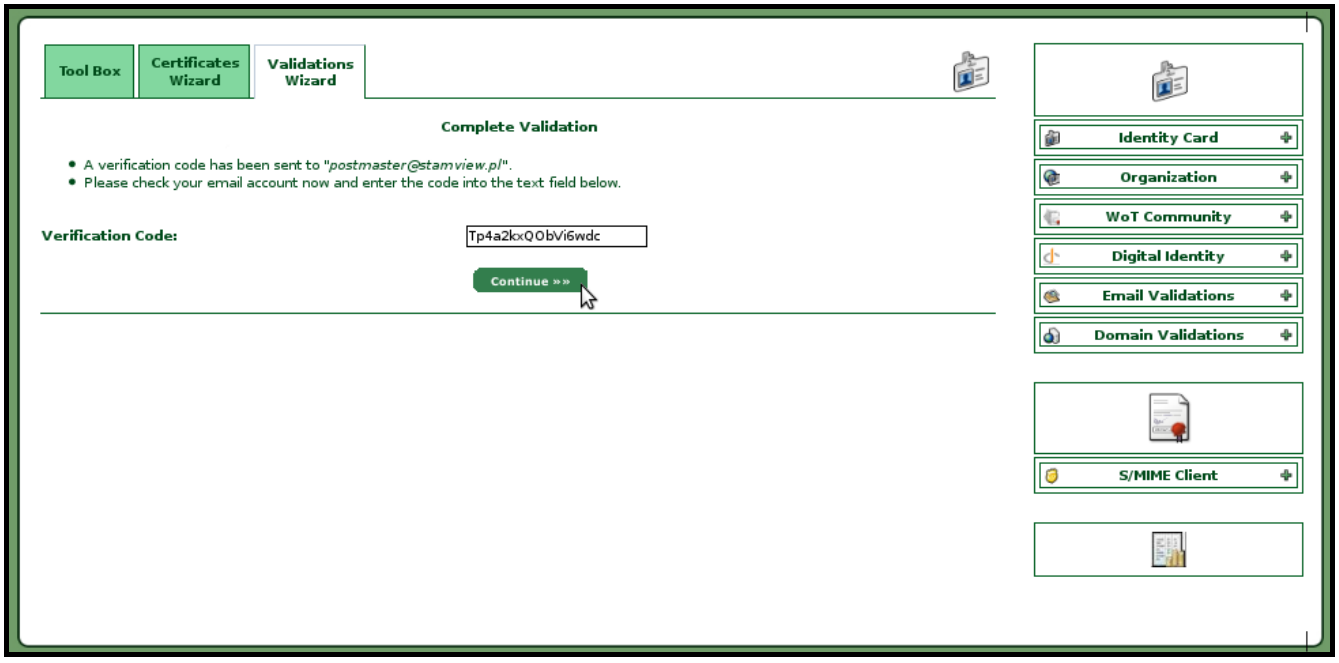
13. Enter the domain name in the "http://" field. Select the correct domain in the field next to it. Click "Continue".



14. Select the email address to which the message with the code to be used in the next step will be sent. In this example, the address is "postmaster@stamview.pl".

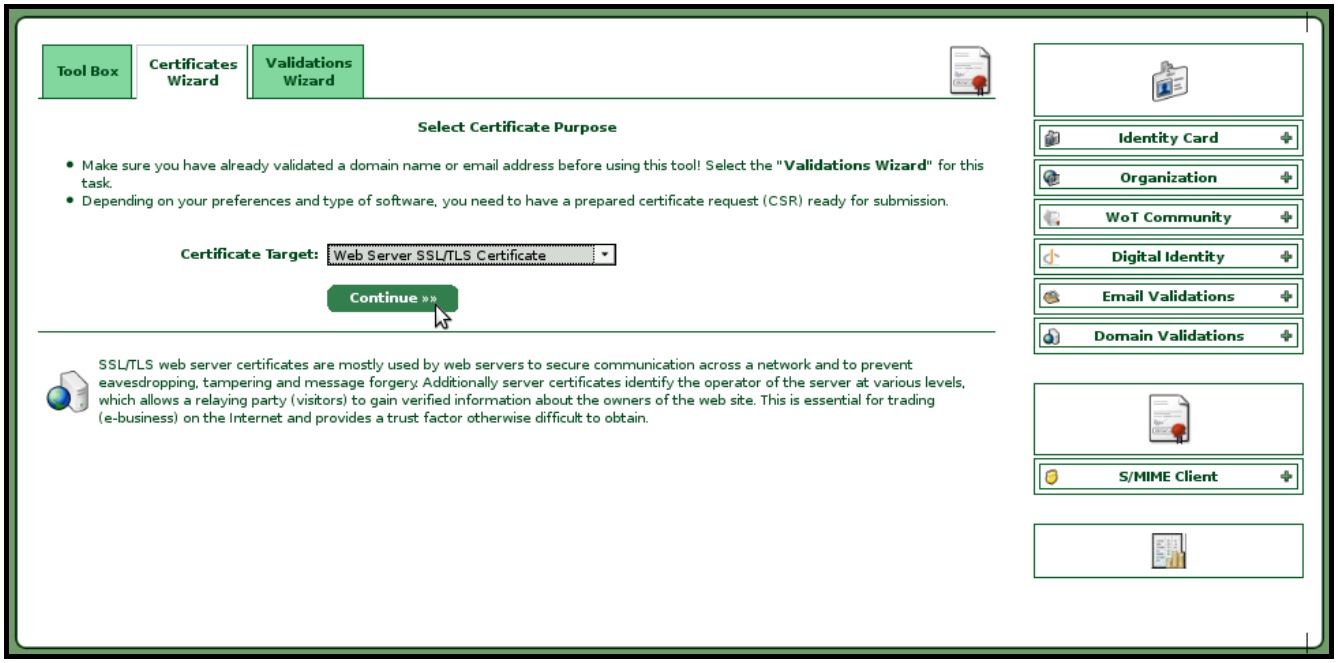


15. In the "Verification Code", enter the code you received in the email message sent to the address indicated in the previous window. Click "Continue".

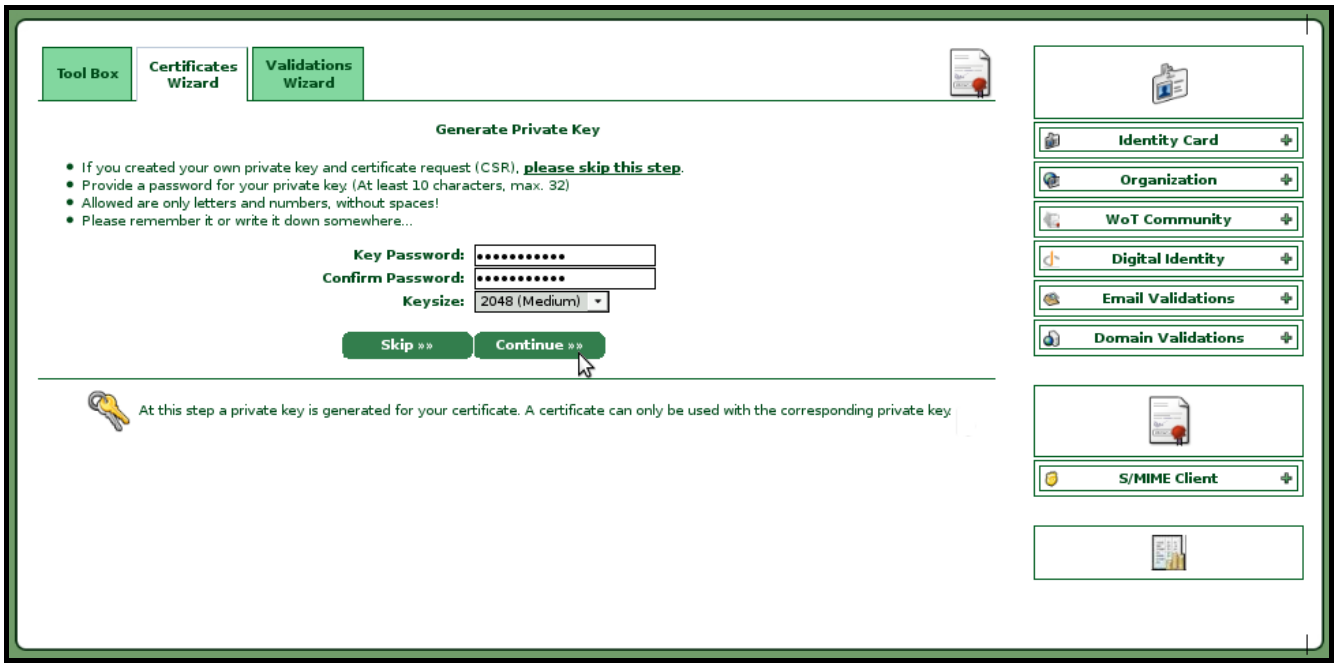


16. Click on the "Finish" button.

17. Click on the "Certificates Wizard" tab. In the "Certificate Target" field, select the "Web Server SSL/TLS Certificate" option and click "Continue".

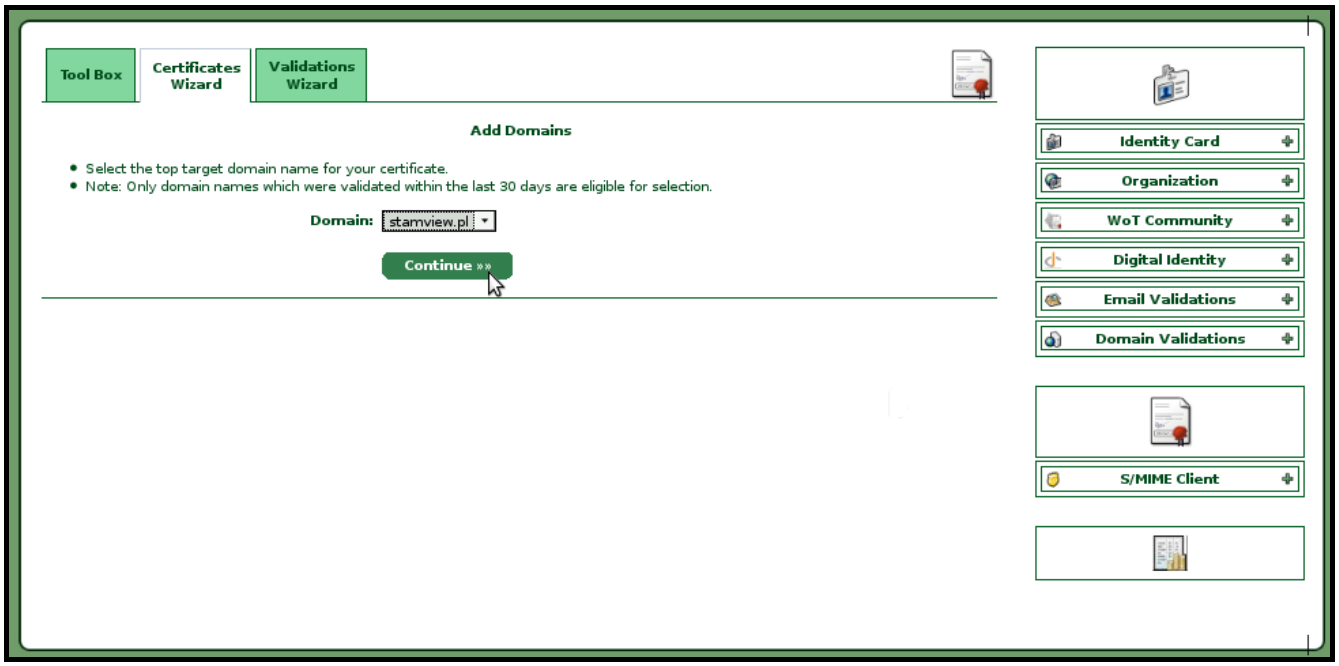


18. Enter your password in the "Key password" field. You can enter from 10 to 32 characters (digits and letters). To confirm the password, type it again in the "Confirm Password" field. Click "Continue".

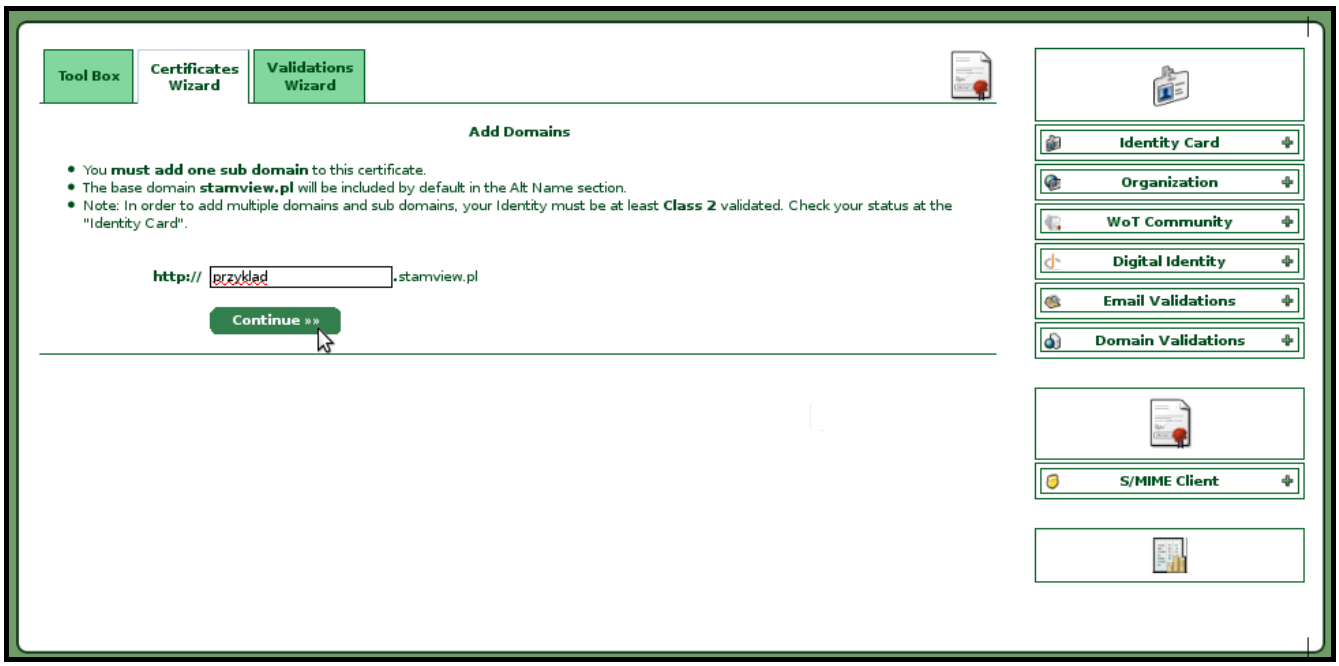


19. Select and copy (Ctrl+C) the text that will appear in the text field. Open the "Notepad" and paste the copied text. Save the file as "ssl.key". Click "Continue".

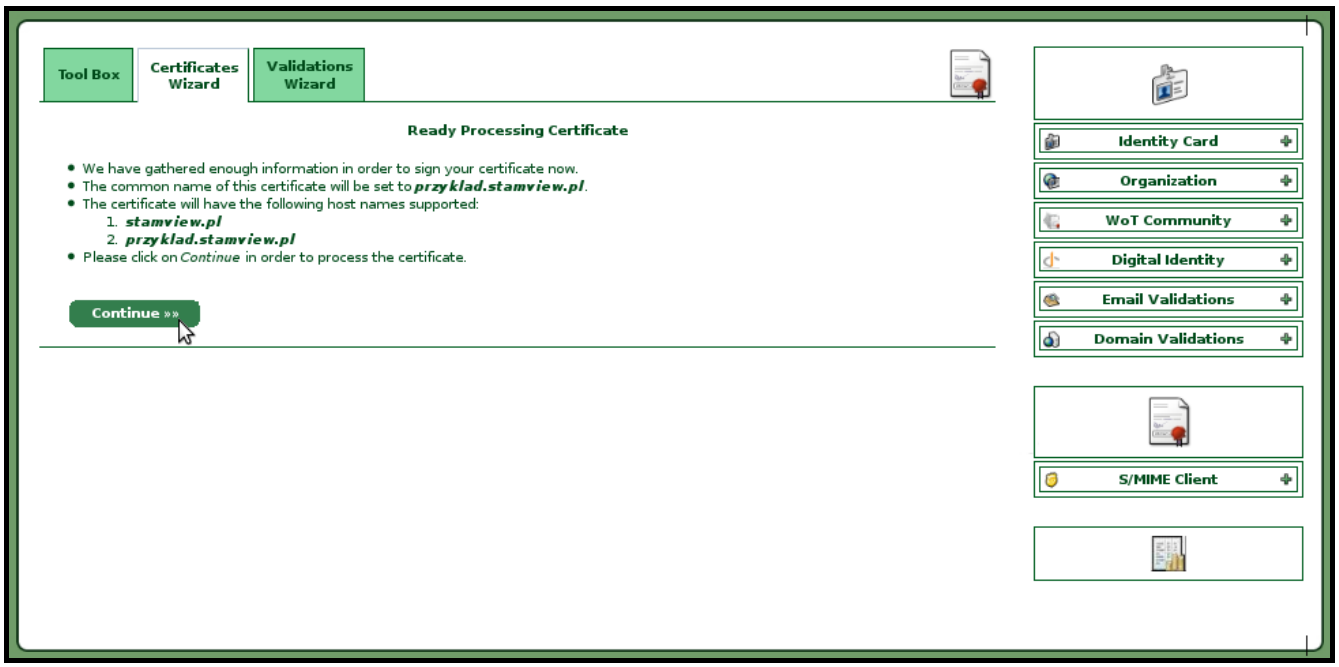
20. Select the name of the previously verified domain in the window that will open. Click "Continue".



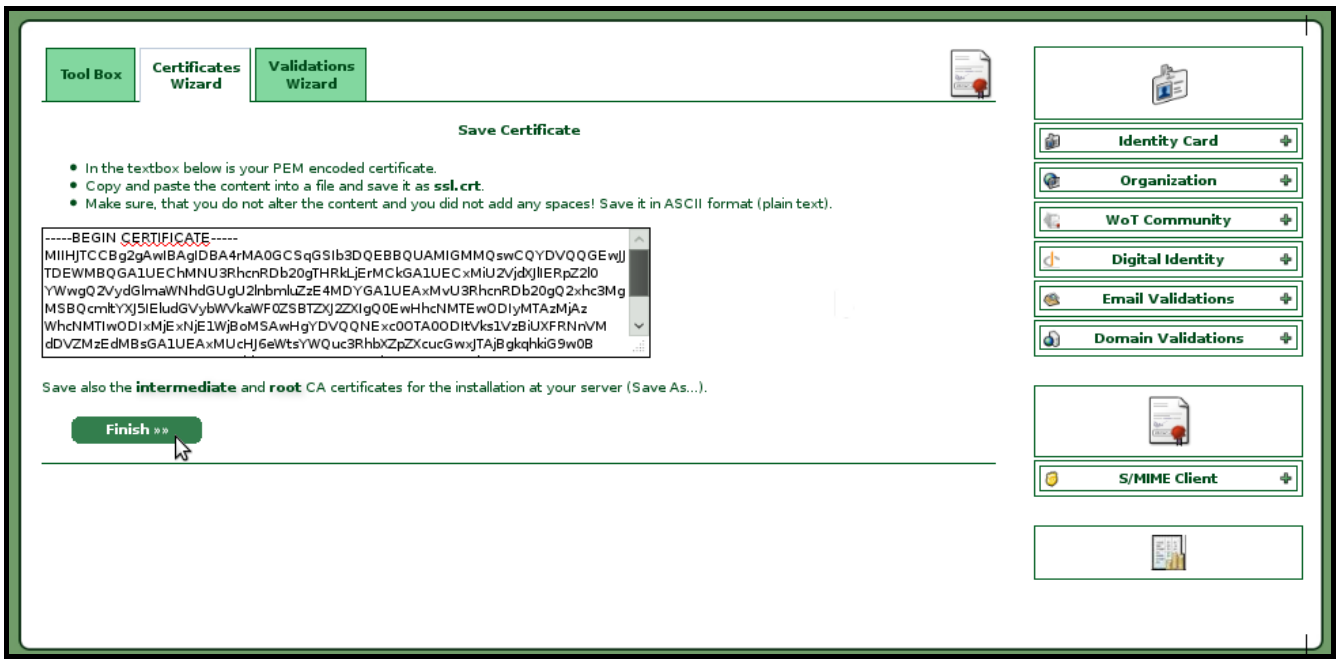
21. Create a subdomain under the previously verified domain. This will be an address of the STAM-VIEW system to which the users will log in. Given in the window below is a sample address: http://przyklad.stamview.pl. Click "Continue".



22. One certificate will be generated, in this case named "przyklad.stamview.pl", common for the domain and subdomains. Click "Continue".



23. Select and copy (Ctrl+C) the text that will appear in the text box. Open the "Notepad" and paste the copied text. Save the file as "ssl.crt". Click "Finish". The "ssl.key" and "ssl.crt" files are prepared to be downloaded into the STAM-VIEW system.



3.1.1 Decrypting the "ssl.key" file

The "ssl.key" file is password encrypterd. If it remains in this form when downloading certificates to the STAM-VIEW system, you will need to enter the password in the appropriate field. You can also decode it in the certificate generating program, immediately after saving the "ssl.crt" file.

In order to decrypt the "ssl.key" file in the certificate generating program, the administrator should perform the following steps:

1. Select the "Tool Box" tab.
2. Select the "Decrypt Private Key" option.
3. In the "ssl.key" file, select the entire text, copy it and paste into the text box that has been displayed in the window.
4. In the "Key password" field, type in the password that was entered when generating the "ssl.key" file (see previous section, it.18) and click "Decrypt".
5. Select and copy (Ctrl+C) the decrypted text which will appear in the text box. Open the "Notepad" and paste the copied text into it. Save the file as "ssl.key", replacing the previously saved file with the same name.

Note: *The free certificates are usually generated for a specified period of time. Please remember to generate them again in due time.*

3.2 Certificates of other certification bodies

Certificates of other certification bodies can also be used. In such a case, the administrator, following the instructions of the individual bodies, must generate files of the relevant certificates, save them to disk and download to the STAM-VIEW system.

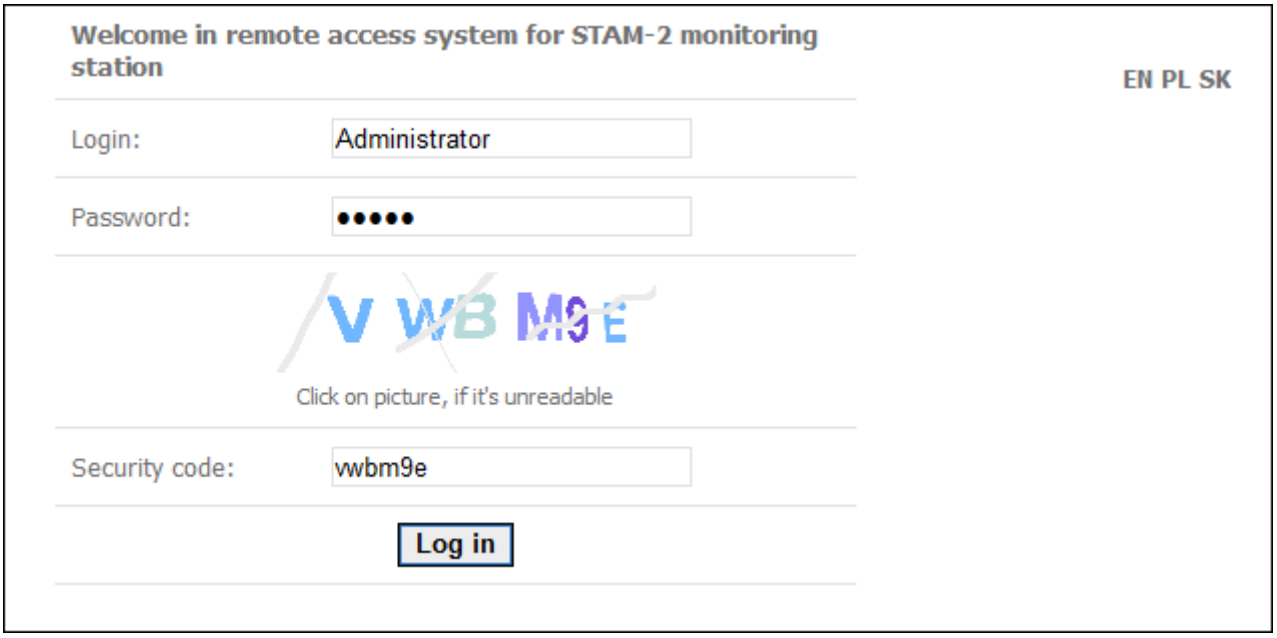
4. System management

The system works with the following web browsers: Mozilla Firefox (recommended), Google Chrome and Internet Explorer from version 8.0.

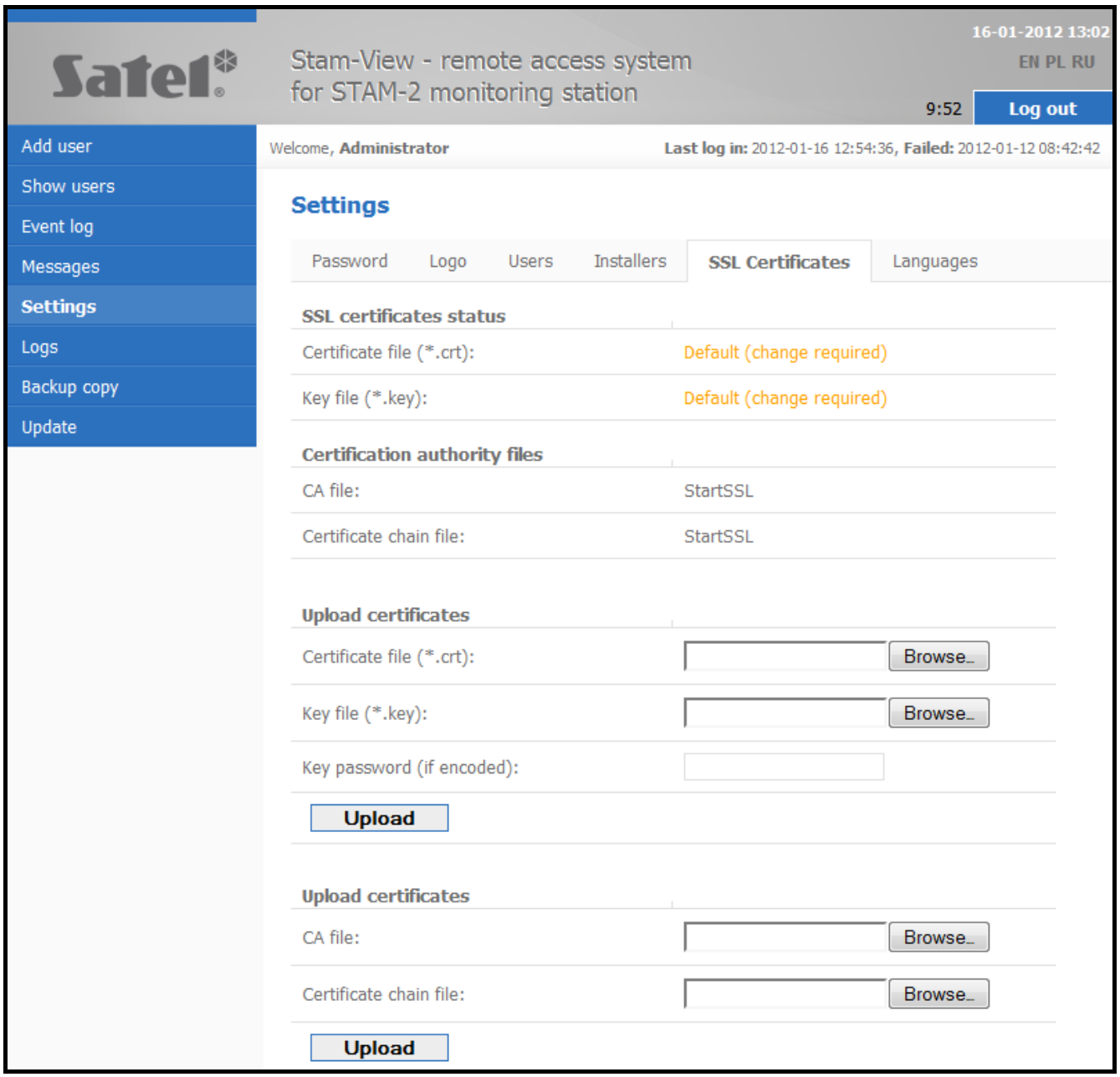
Note: *No activity for 10 minutes will result in logout from the system. Each click to select another tab will restart the countdown.*

4.1 First login

1. Enter the address **http://[STAM-VIEW virtual machine address]** in your web browser on the computer connected to the LAN to which the VMWare ESXi server is connected. The address can be entered in the form of an IP address (4 decimal numbers separated by dots) or in the form of a domain name.
2. Log in to the system (enter the login, password and code from the picture). By factory default, the **Administrator** login and the **satel** password are preprogrammed for the administrator in the system.



3. Enter the "Settings" tab and select the "SSL Certificates" in it.
4. When generating the StartCom SSL certificates, click the "Browse ..." button in the "Certificate file (*.crt)" field and select the previously saved "ssl.crt" file. In the "Key file (*.key)" field, click the "Browse..." button and select the previously saved "ssl.key" file. If the key file is still encrypted, enter the password you gave when generating the "ssl.key" file in the "Key password (if encoded)" (see the system installer manual). Click the "Upload" button.
5. When generating the SSL certificates of another certification body, click the "Browse..." button in the "CA file" field and select the appropriate file. Click the "Browse..." button in the "Certificate chain file" field and select the appropriate file. Click the "Upload" button.
6. After the certificate and the key have been accepted, the status of SSL / authorizing body certificates in both fields will change to "OK".



4.2 Next logins

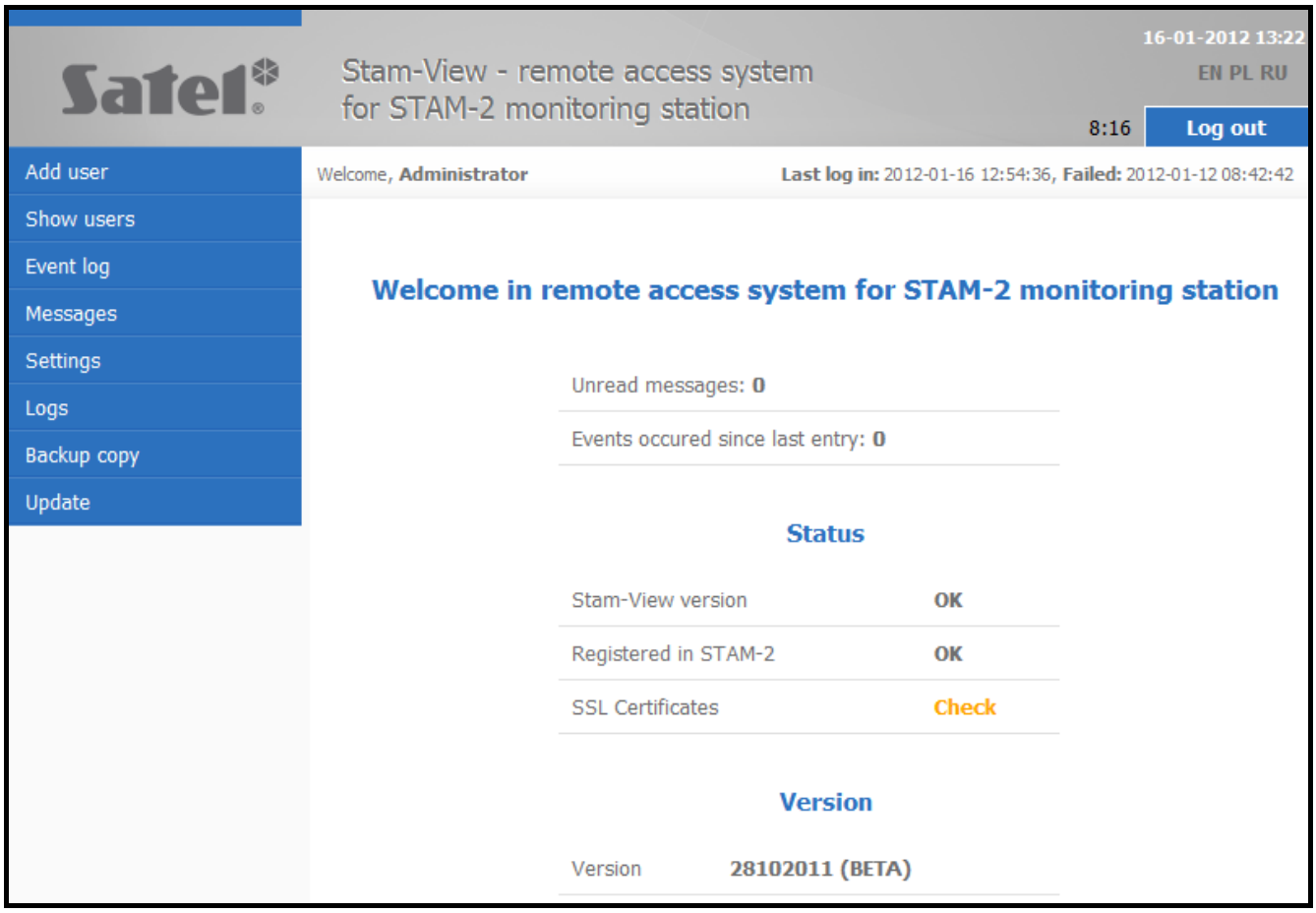
In order to get access to the STAM-VIEW system, enter the address **https://[address of the STAM-VIEW virtual machine]** in the browser. The address can be entered in the form of an IP address (4 decimal numbers separated by dots) or in the form of a name.

4.3 Changing password

The factory default password should be changed after first login to the system. The administrator, in order to change the password, should perform the following steps:

1. Click on the "Settings" button.
2. Click on the "Password" tab.
3. Enter the old password and the new one (the new password has to be confirmed). Press the "Change password" button to confirm the change made.

4.4 Information displayed after login



Each time after you have logged in to the system, the following information is displayed: the time of the last successful and failed login attempts, the number of unread messages, the number of events that have been received by the monitoring station since the last login, the software version, the status of communication between the STAM-VIEW system and the monitoring station, and the status of SSL certificates. In the event of any inconsistency, information in red color will appear at each of the statuses.

If a red "Update required" message appears at the "Stam-View version" field, the system administrator must update the STAM-VIEW version. Download the appropriate update file from the www.satel.eu website and save it to disk. Then enter the "Update" tab and click the "Click here to update" command in it. In the "Update file" field, enter the access path to the downloaded file.

If a red "No" message is displayed at the "Registration in STAM-2" field, the monitoring station operator should select the "Enabled" option in the STAM-2 program, "Configuration" window, "Settings" tab, then fill correctly the fields required for a valid connection, and click "Apply". Then quit the STAM-2 Server program and restart it. After the STAM-VIEW system receives data from the monitoring station, the "OK" message will be displayed in the window.

If a red "No" message is displayed at the "SSL Certificates" field, you should download the certificates again to the STAM-VIEW system. The administrator should enter the "Settings" tab and the "SSL certificates" tab in it. The red "No" message will be displayed at the SSL certificates and the authorizing body certificates. Use the "Upload" button to download the corresponding certificate files.

4.5 Changing logo

An option is provided to substitute the logo displayed at the top of the system window. In order to do it, the administrator should perform the following steps:

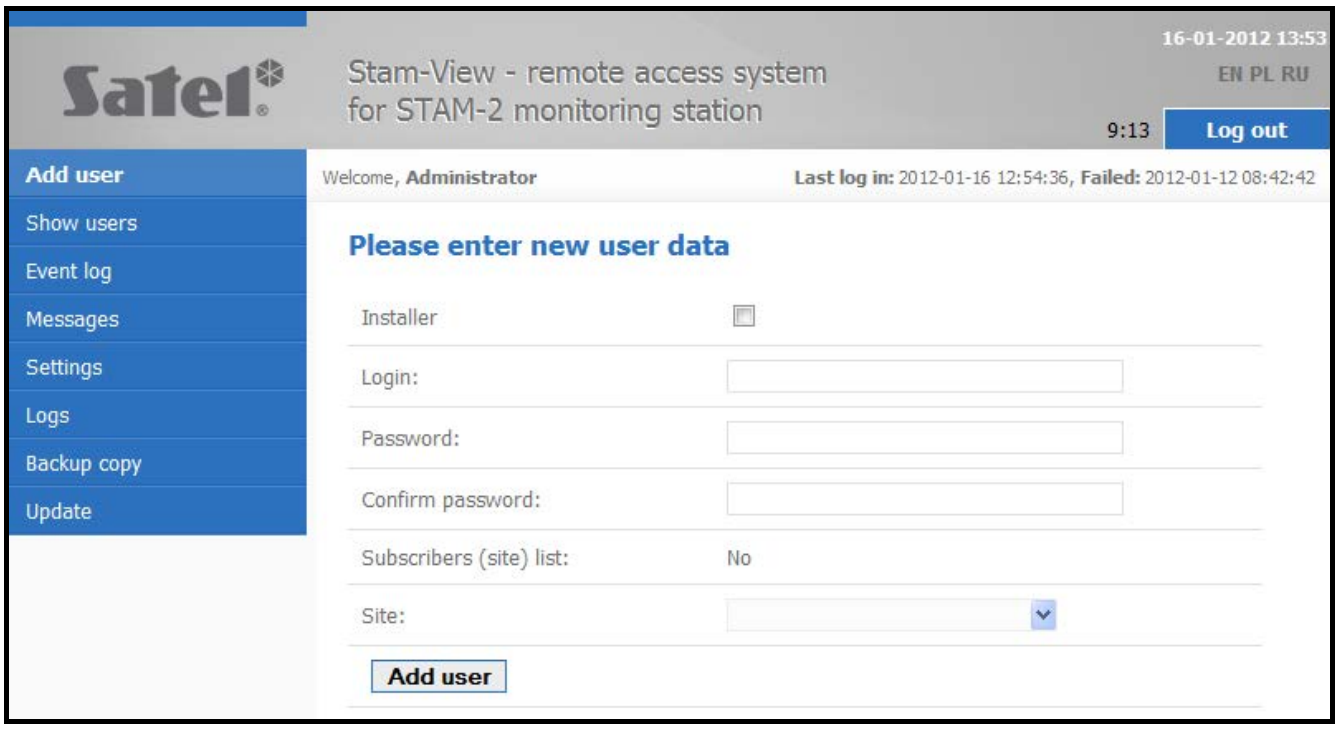
1. Log in to the system.
2. Enter the "Settings" tab and then the "Logo" tab in it.
3. Click the "Browse" button and select the file with preselected logo.

Note: *The system accepts only the files of PNG, BMP and GIF type, with a resolution of 200 x 74 pixels.*

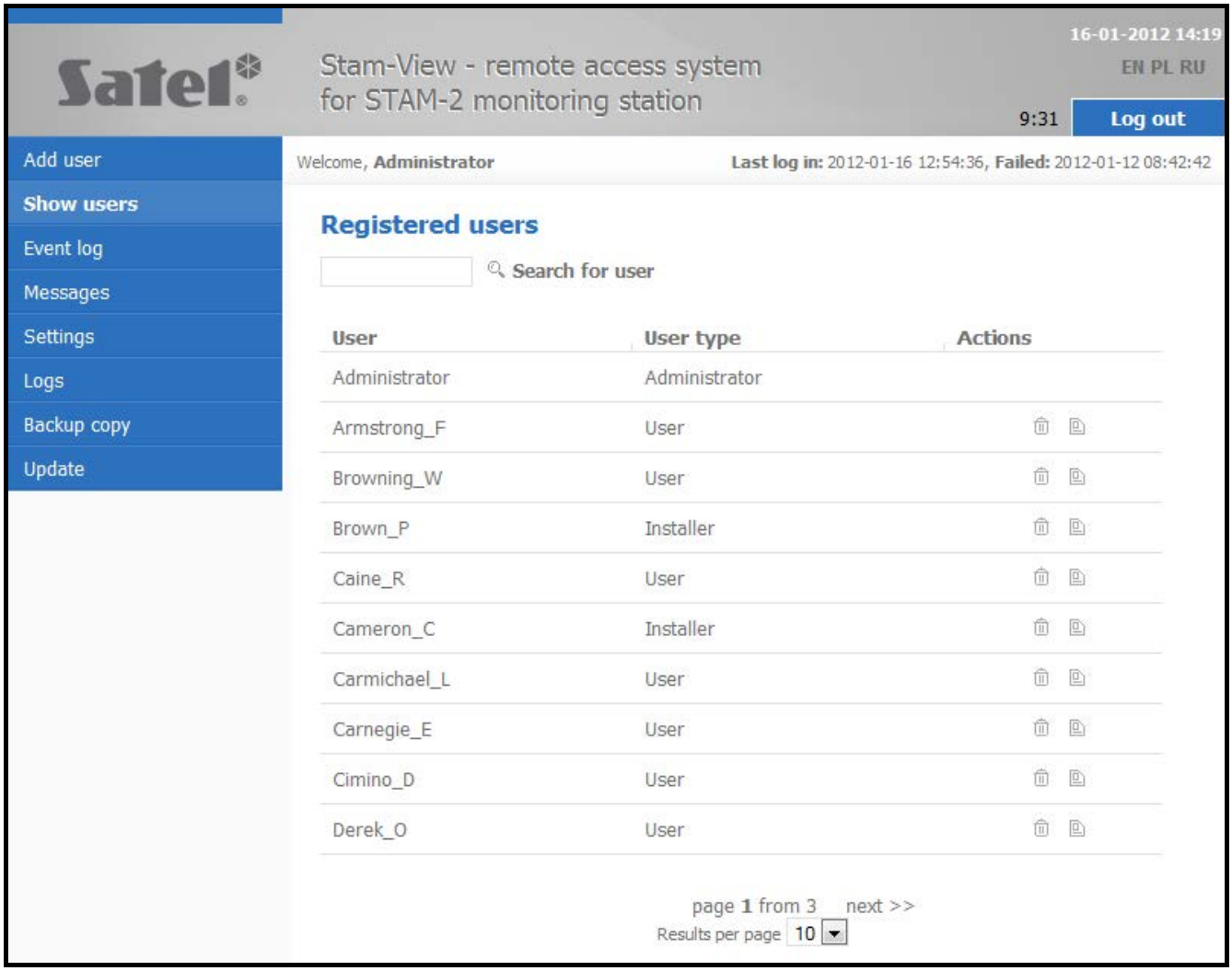
4. Click on the "Change logo" button.
5. Determine position of the image and align it horizontally and vertically using the appropriate buttons.

4.6 Administrator permissions in the system

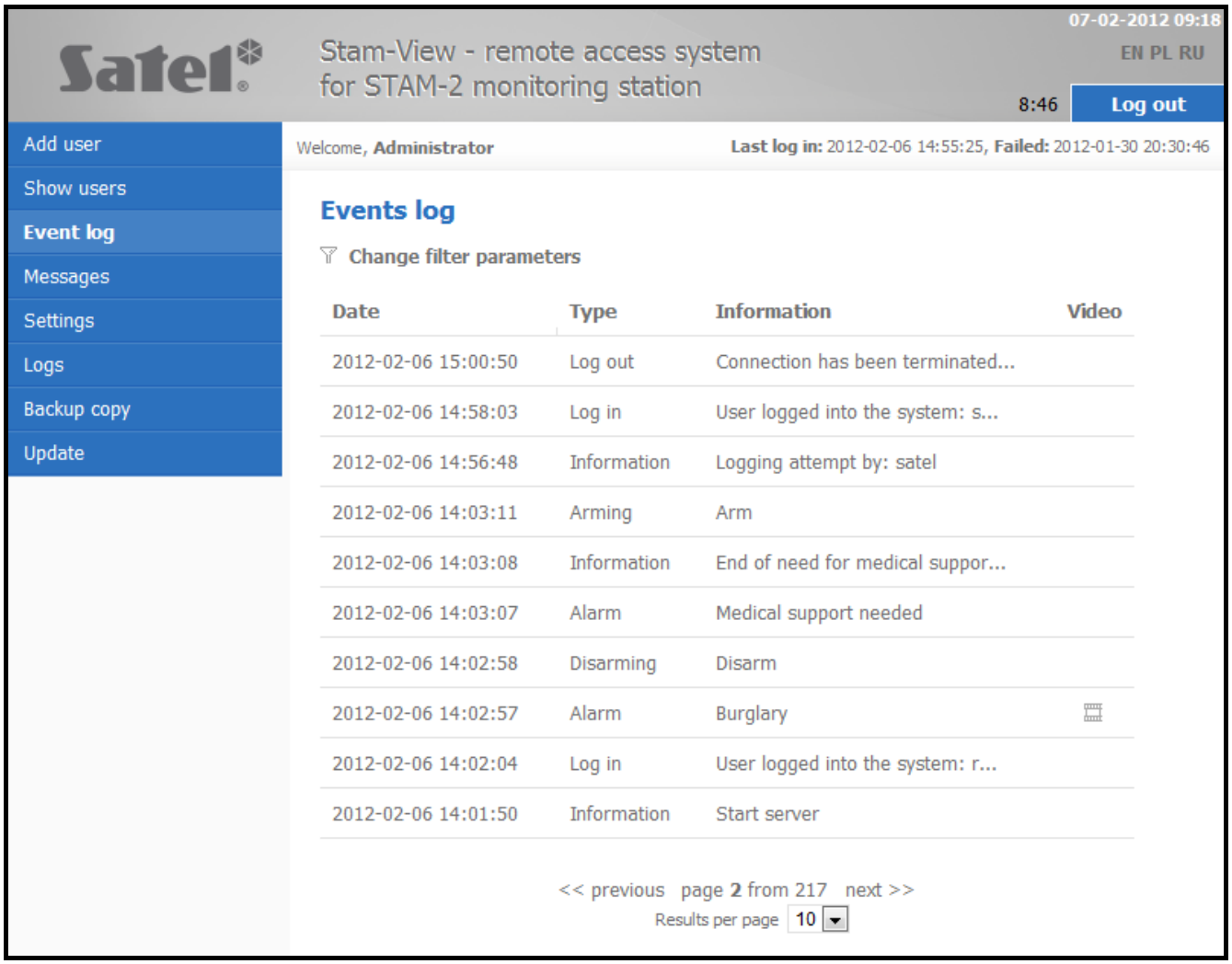
1. Adding, editing and deleting users (the passwords can contain from 4 to 16 characters).
2. Assigning permissions to the users.



3. Ability to search for users by their name.

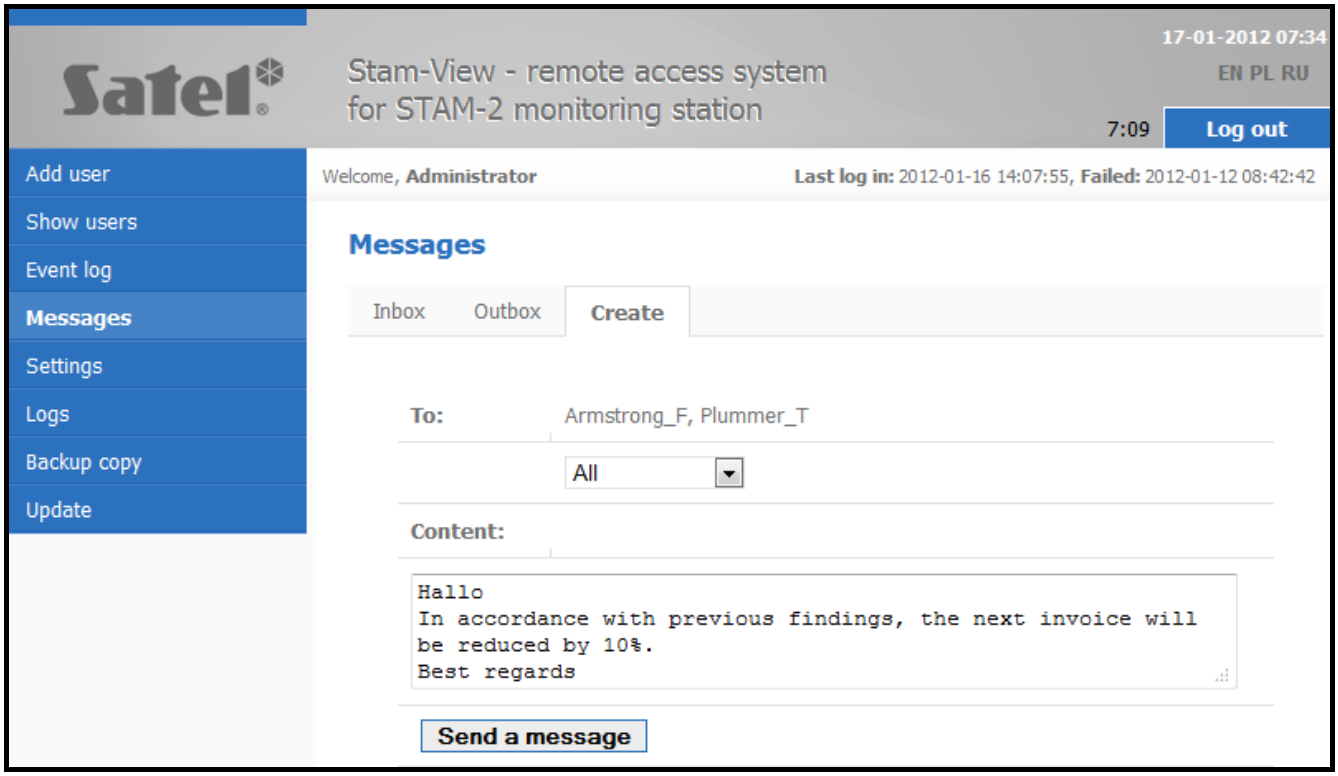


4. Filtering events in accordance with the following criteria:
   - all or selected,
   - for a selected period of time,
   - for a selected subscriber (with a specific login, ID number or name), or all subscribers,
   - containing the text entered,
   - with video confirmation.

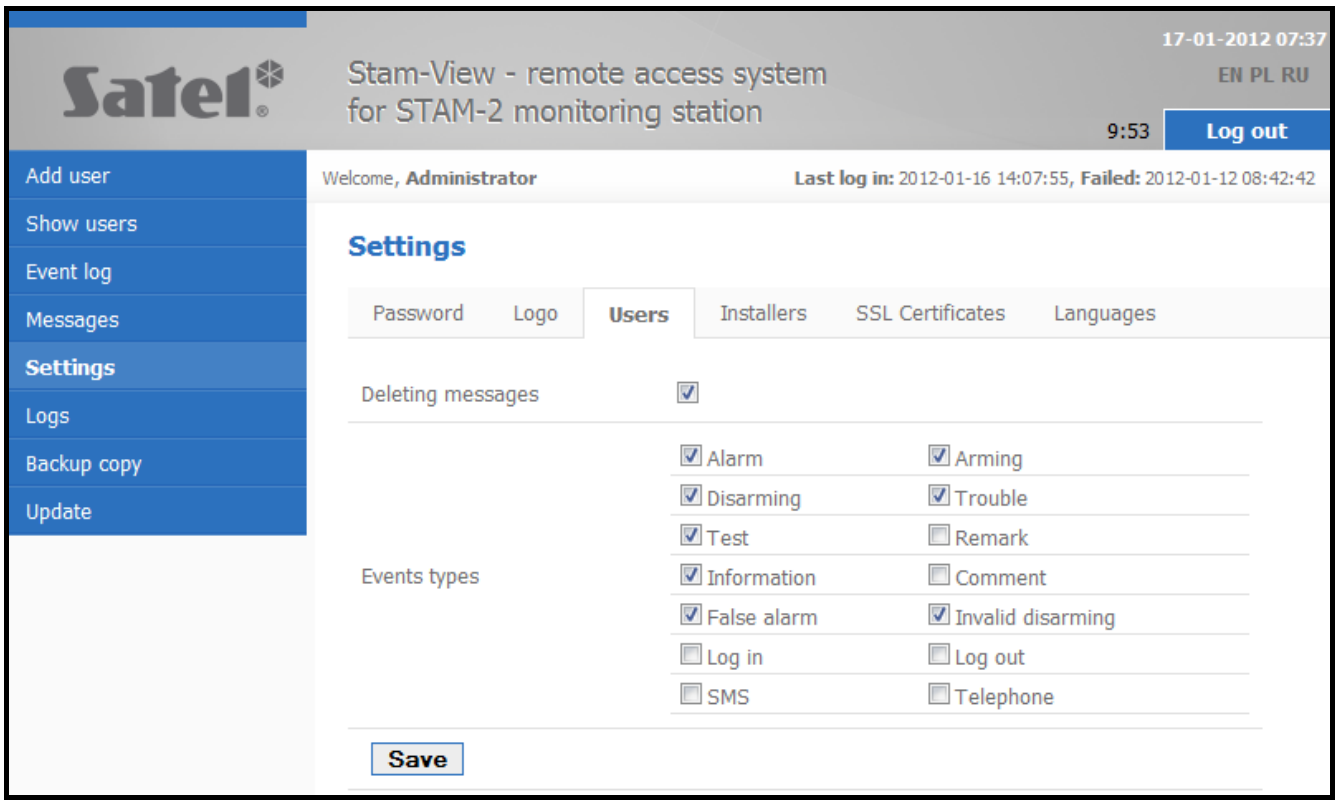


5. Viewing detailed events.

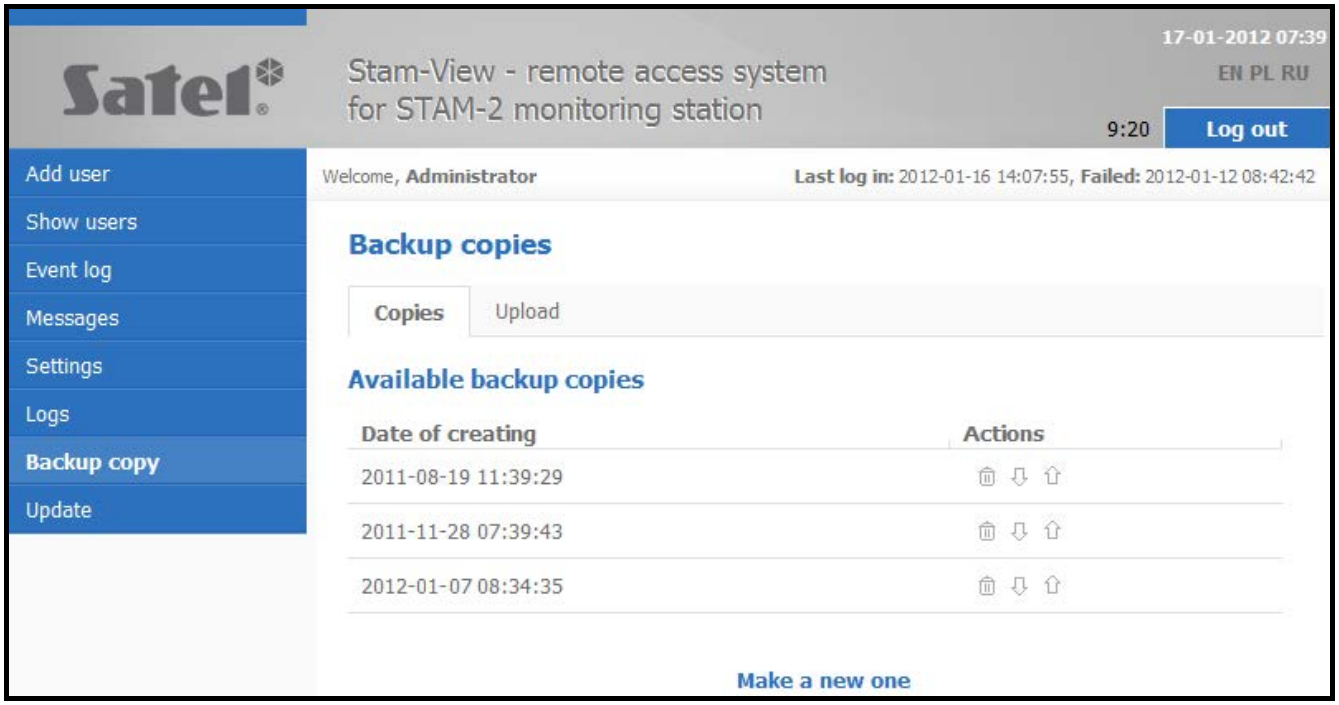
6. Ability to communicate with the installers and users by means of a system of messages.



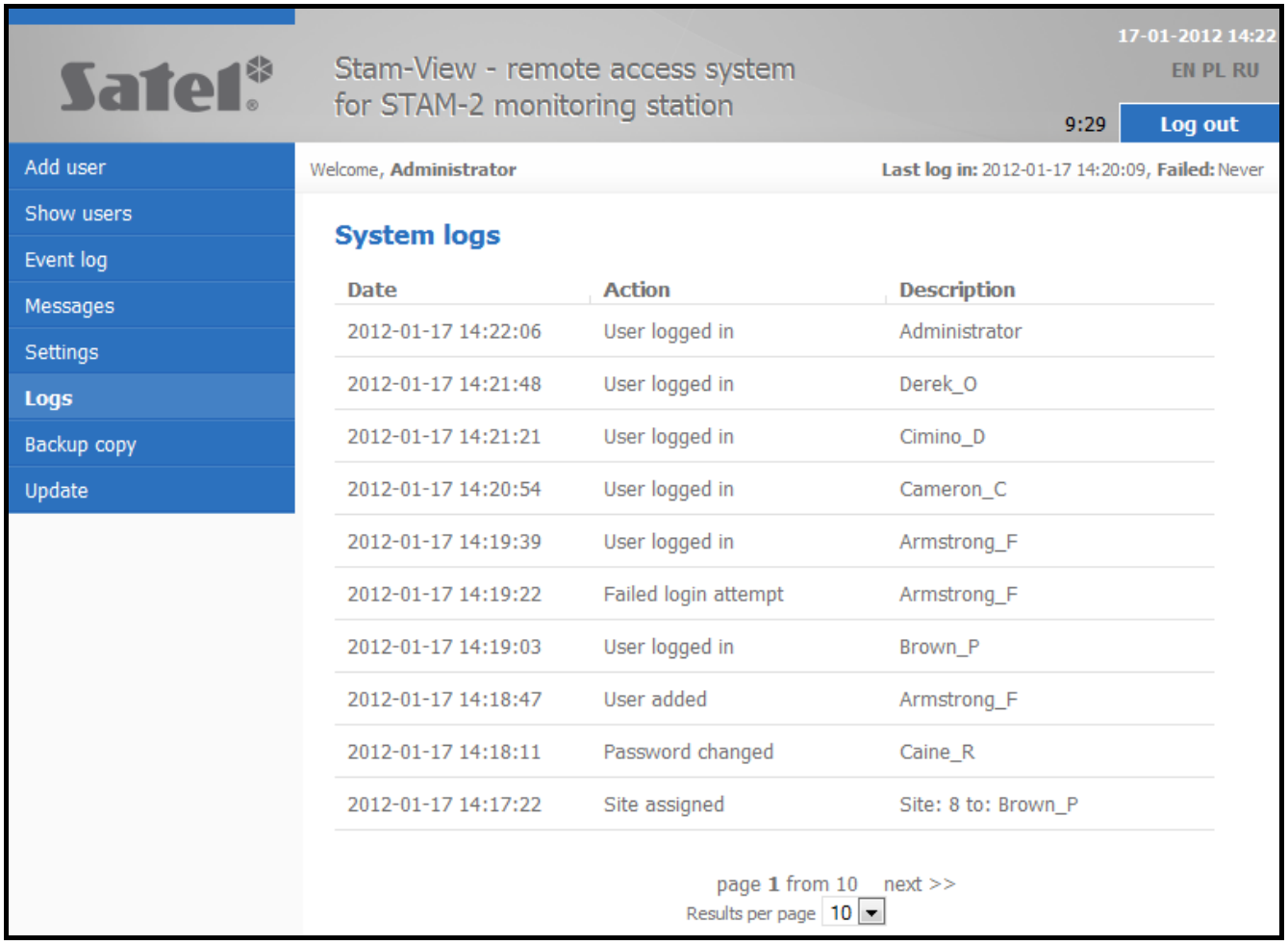
7. Configuration of the STAM-VIEW system settings:
   - optional change of password,
   - optional substitution of the logo displayed at the top of the system window (by default, SATEL's logo is displayed there),
   - defining permissions for all users,
   - defining permissions for all installers,
   - downloading SSL certificates,
   - selection of three languages the system users will be permitted to use,
   - selection of the default language for all users.



8. Ability to make back-up copies of the STAM-VIEW system settings, save them on disk in the STAM-VIEW system database, and restore the saved system configuration.



9. Viewing the STAM-VIEW related system events.



10. Updating the STAM-VIEW system.