

**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

---

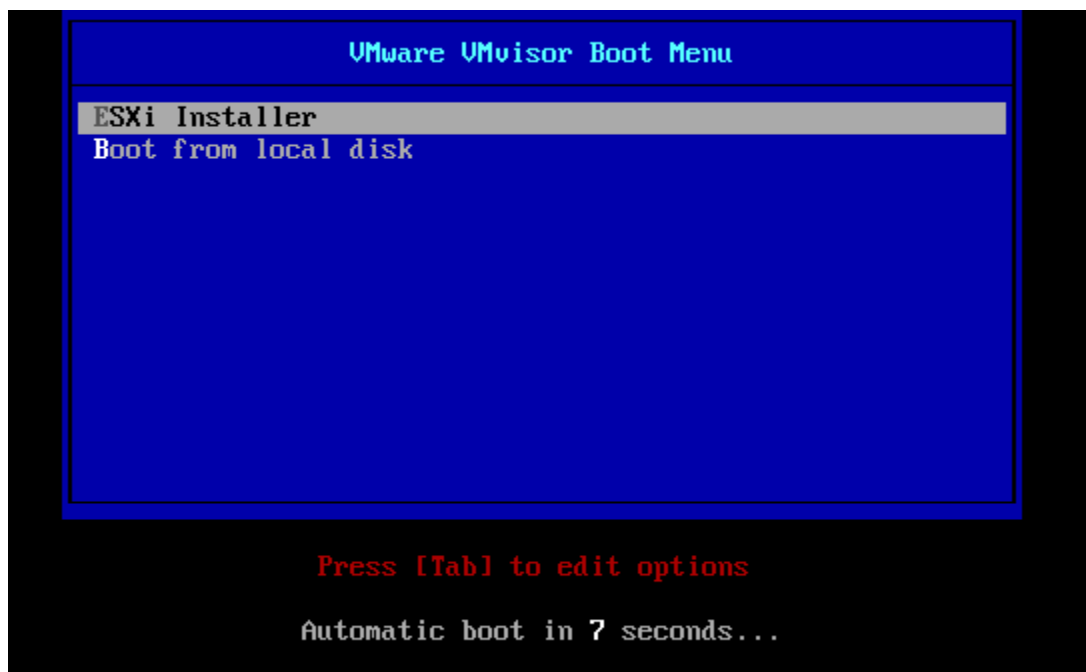
Open the manufacturer's website at <http://downloads.vmware.com/>, select the VMware vSphere Hypervisor (ESXi) item and click on the "Download" button. A page for database registration (enrollment) will be displayed. The registration is required for free downloading of files and getting of a free license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

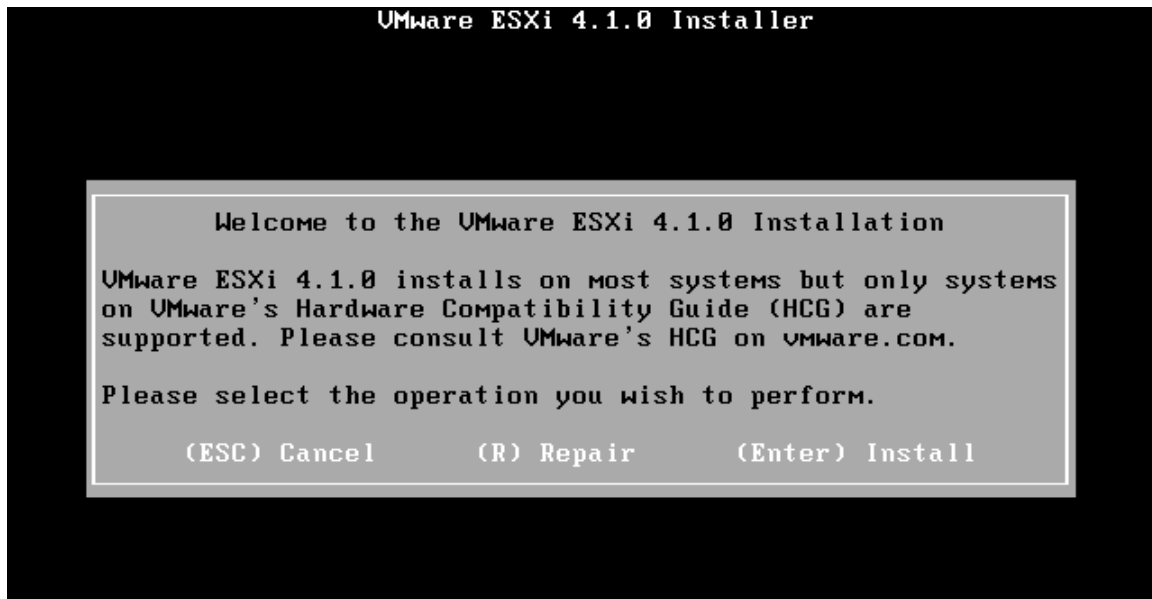
## 2.4 Installation of VMware ESXi operating system

---

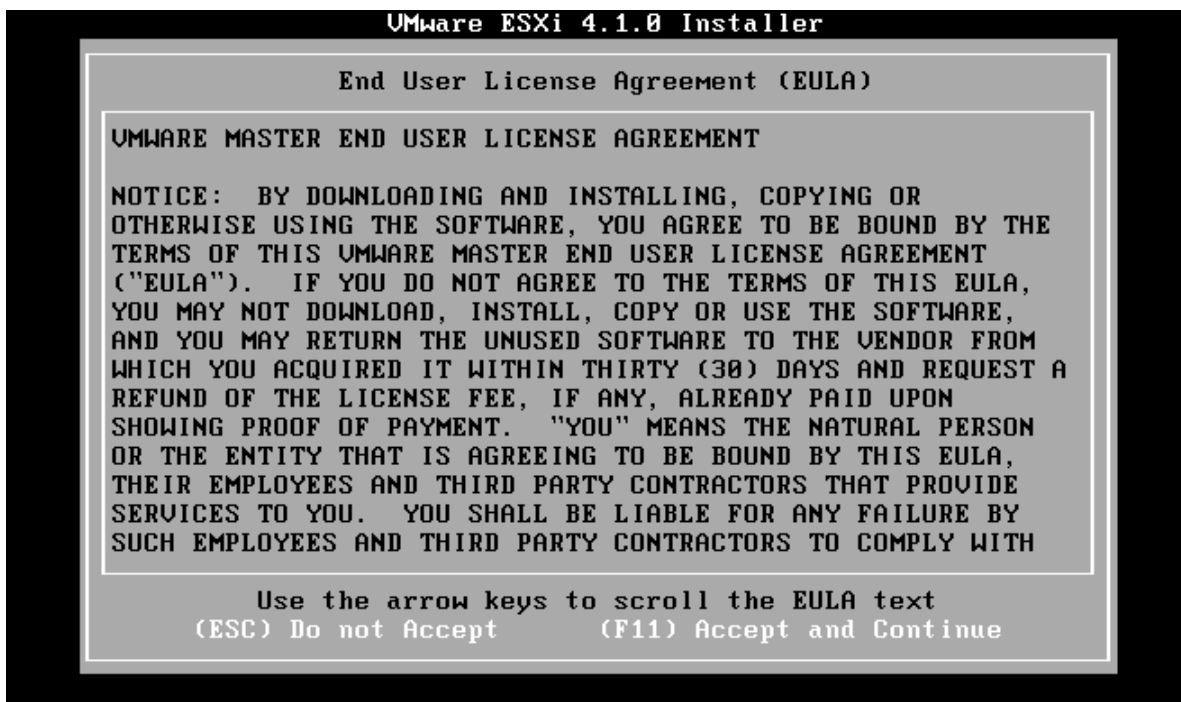
1. Turn on the server and insert the recorded CD into the drive.
2. Select the ESXi Installer option and confirm by pressing ENTER.



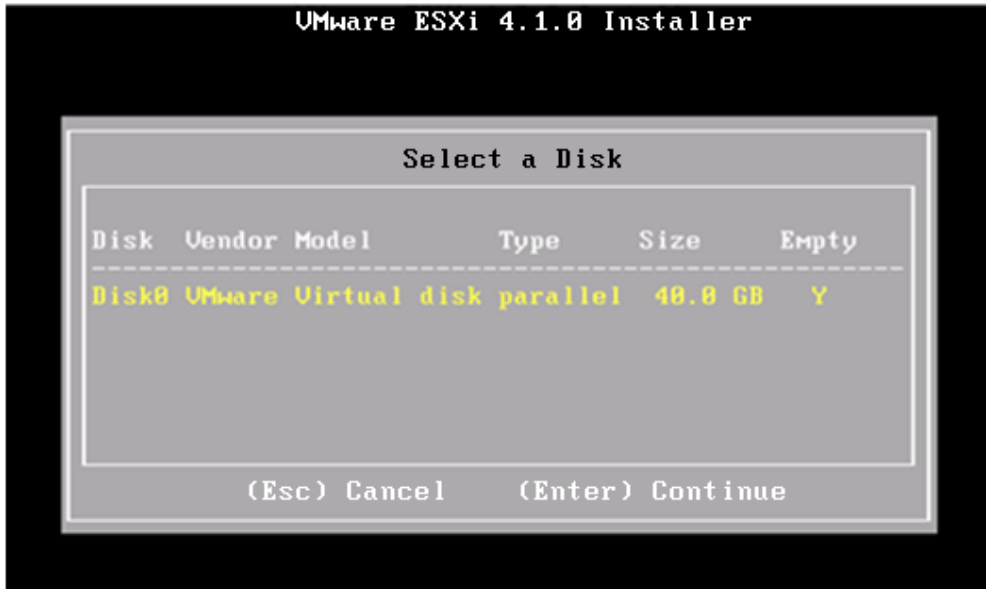
3. A message will be displayed to inform you that the system may only be installed on the hardware which meets the requirements listed earlier in this manual. Press ENTER to continue the installation.



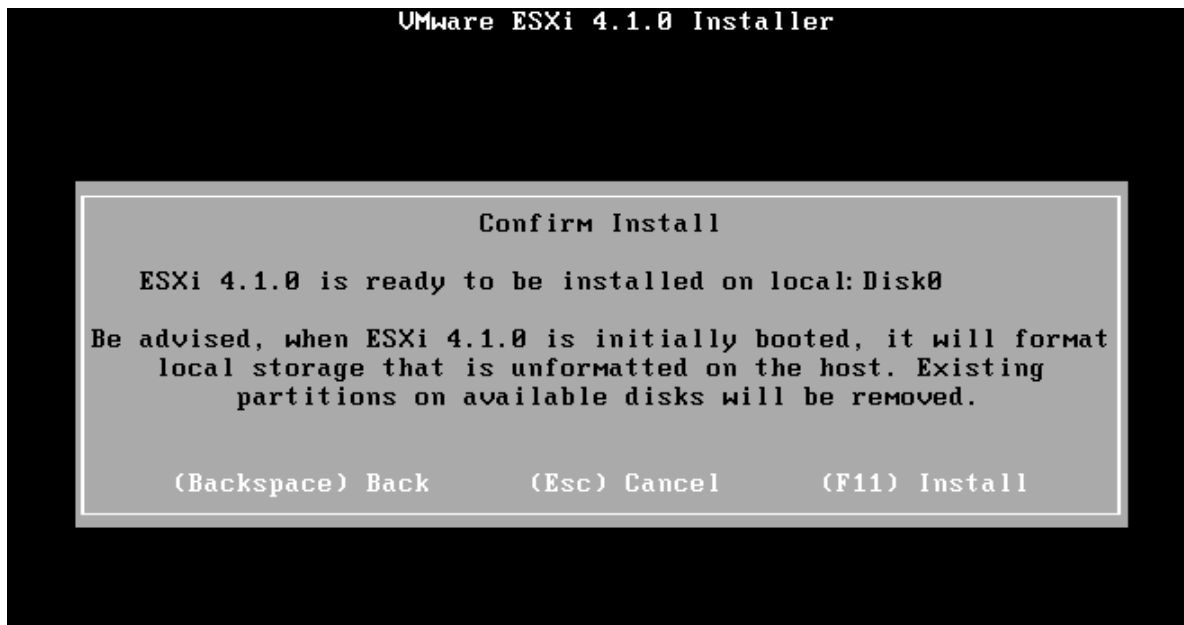
4. After reading the license terms, press F11 to accept them.



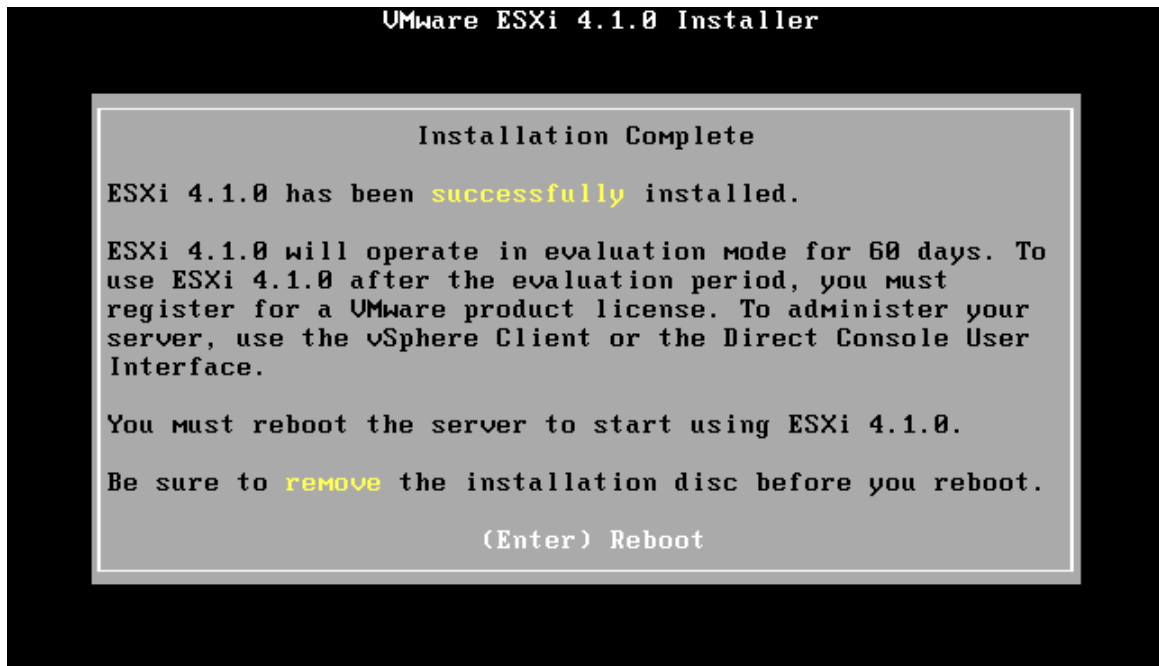
5. A list of drives available on the server will be displayed. Select that on which you want to install the operating system and confirm by pressing ENTER.



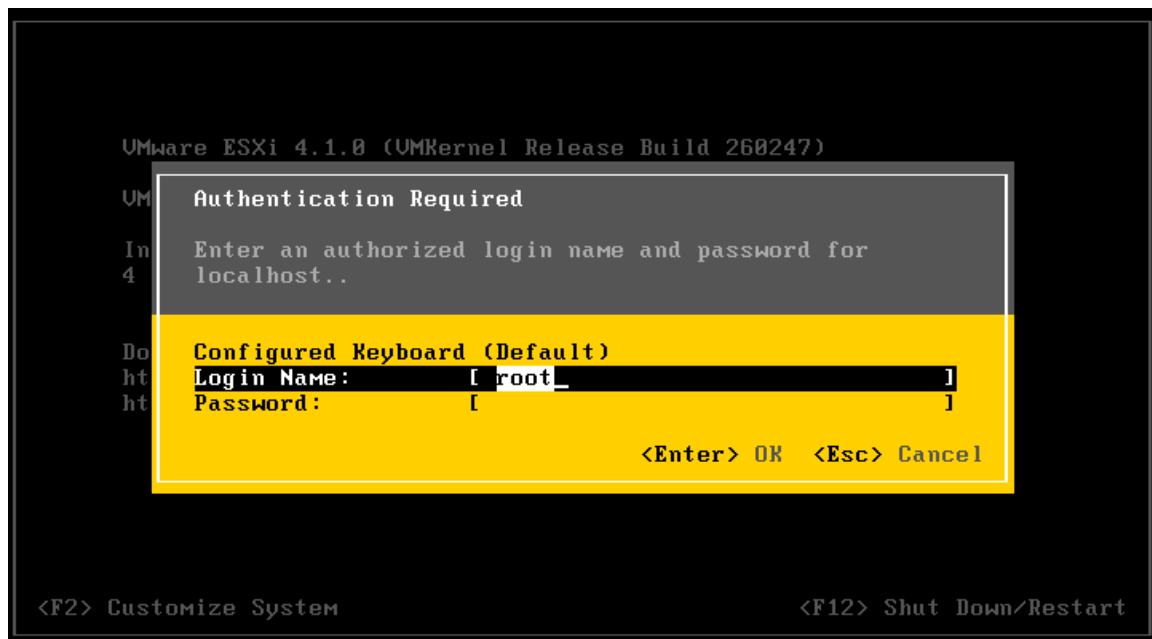
6. Press F11 to start the next installation steps.



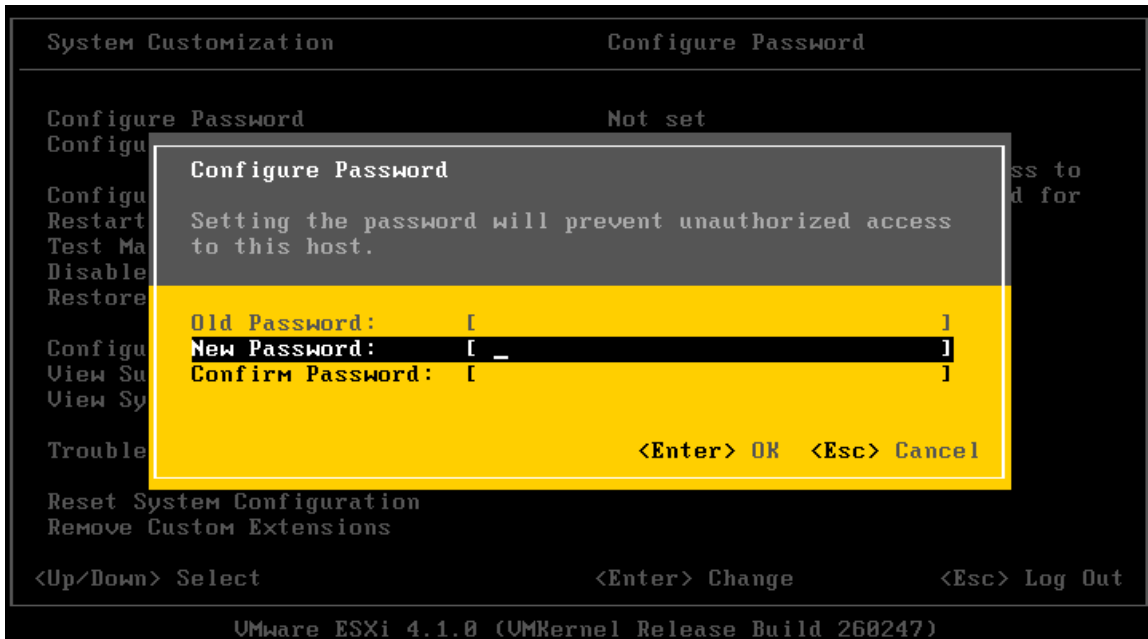
7. Having completed the installation, remove the CD from the drive, and then press ENTER to restart your computer.



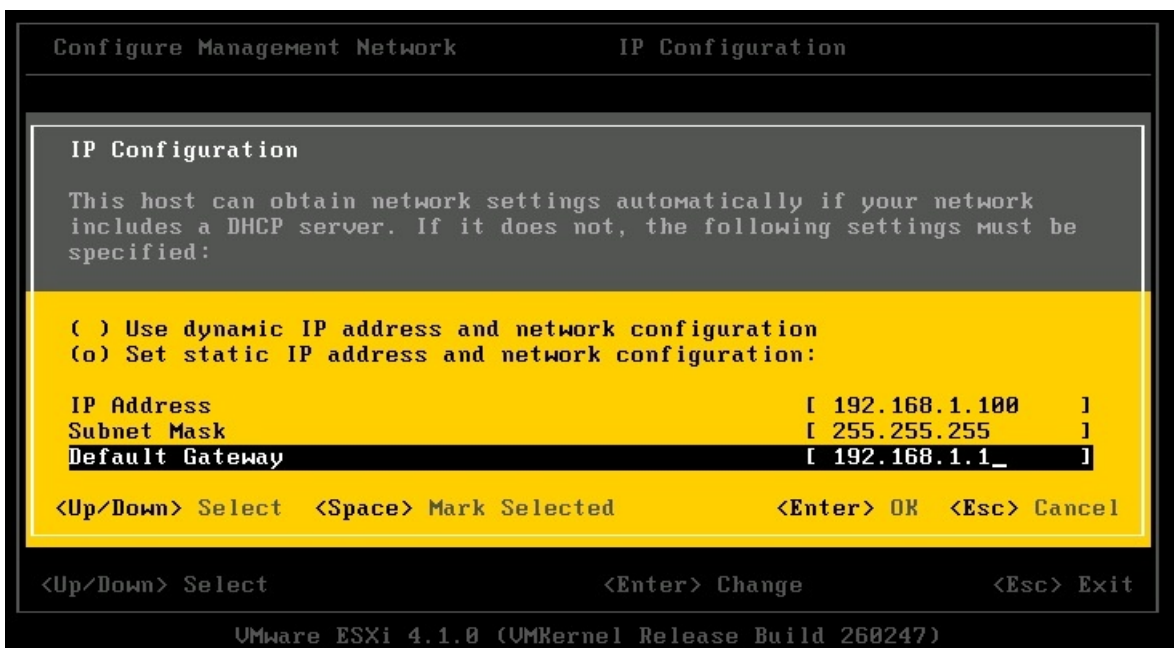
8. After installing the VMware ESXi operating system and rebooting the computer, the "Authentication Required" window will be displayed. Press ENTER to accept the already entered data and go to the next window.



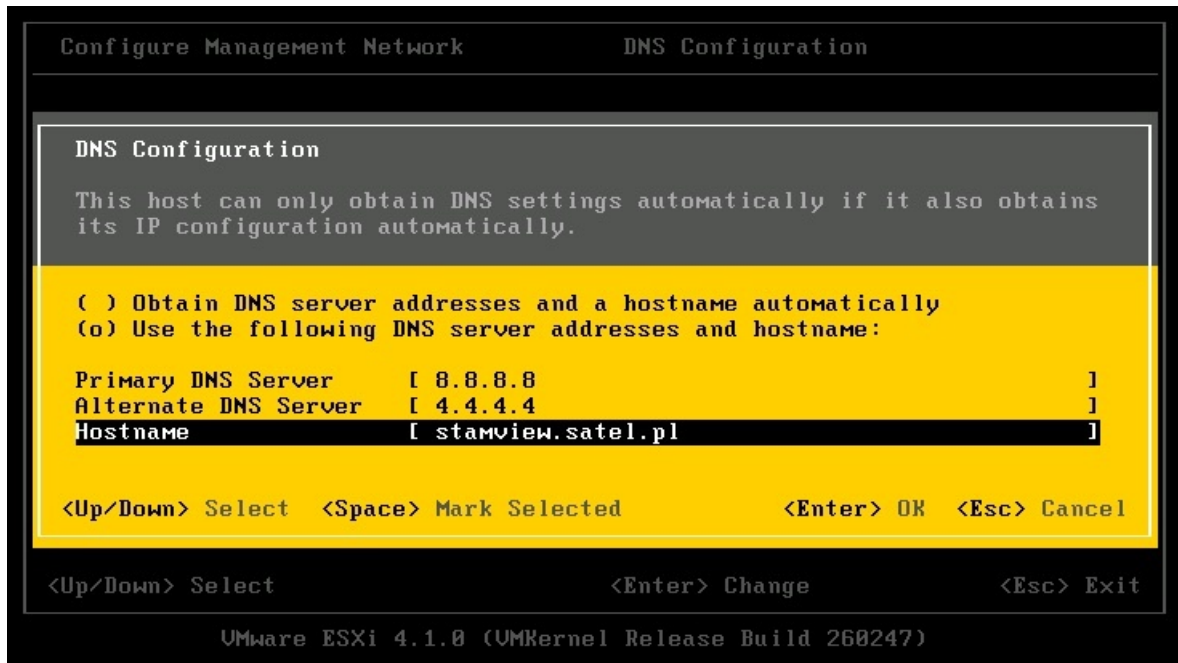
- 9. Press F2 to go to the basic configuration of the server and its network settings. Choose "Configure Password" and define a password for the server. The password can contain from 8 to 40 characters (letters and digits). Confirm your changes by pressing ENTER. Press ESC to go back to the server settings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



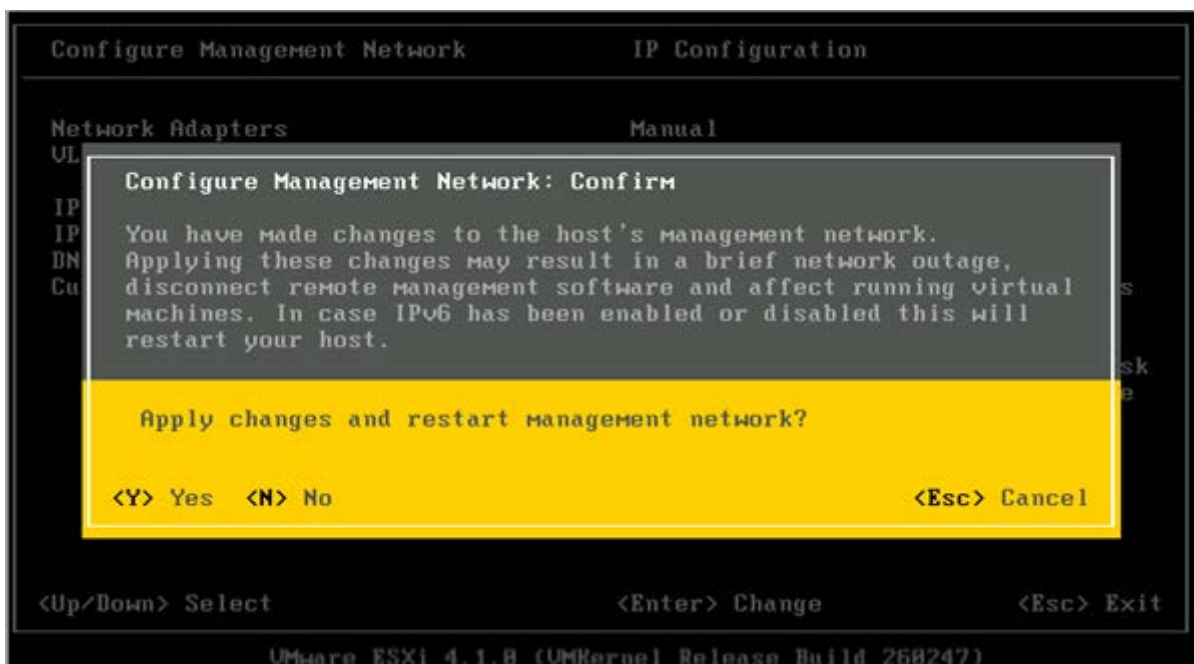
- 10. Select the "Configure Management Network" command, and the "IP Configuration" in it. If the network address is assigned dynamically by the server to the DHCP server, leave the "Use dynamic IP address and network configuration" option selected. If the server's network address is to be entered manually, 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.

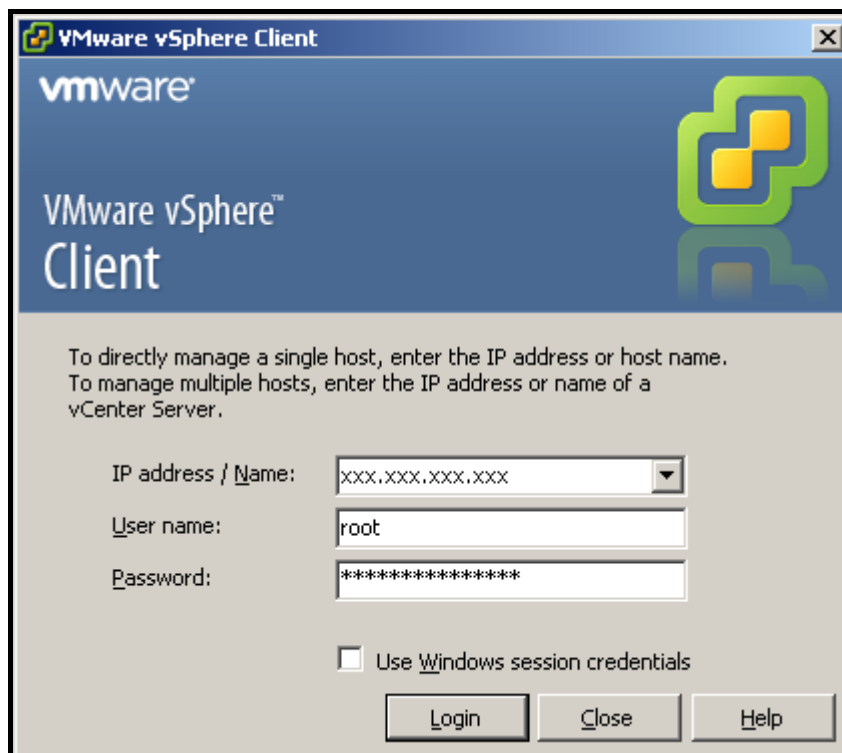


12. Having entered the network data, press ESC to exit the menu, and then press "Y" to confirm the new settings.

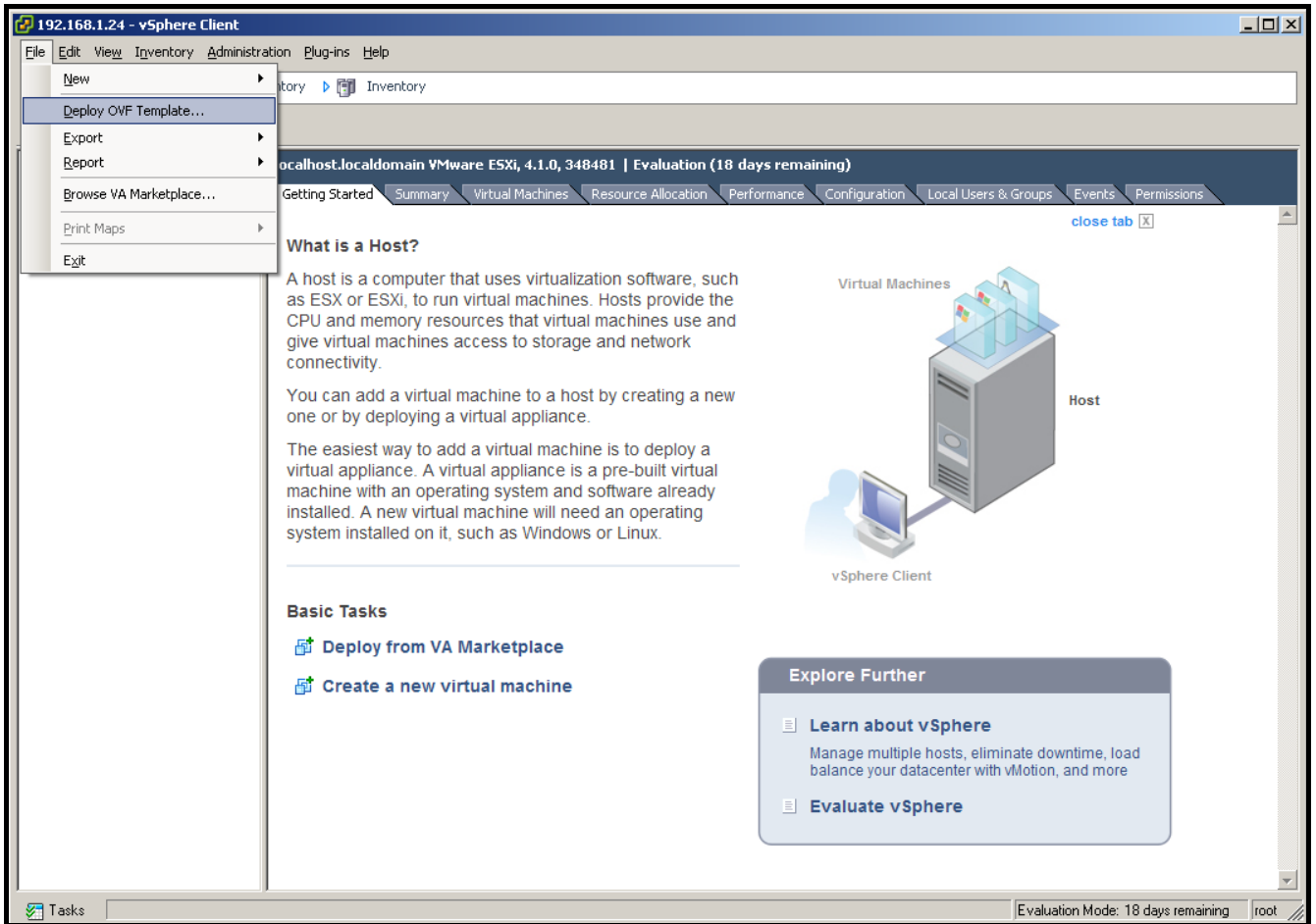


## 2.5 Installation of VMware vSphere Client program

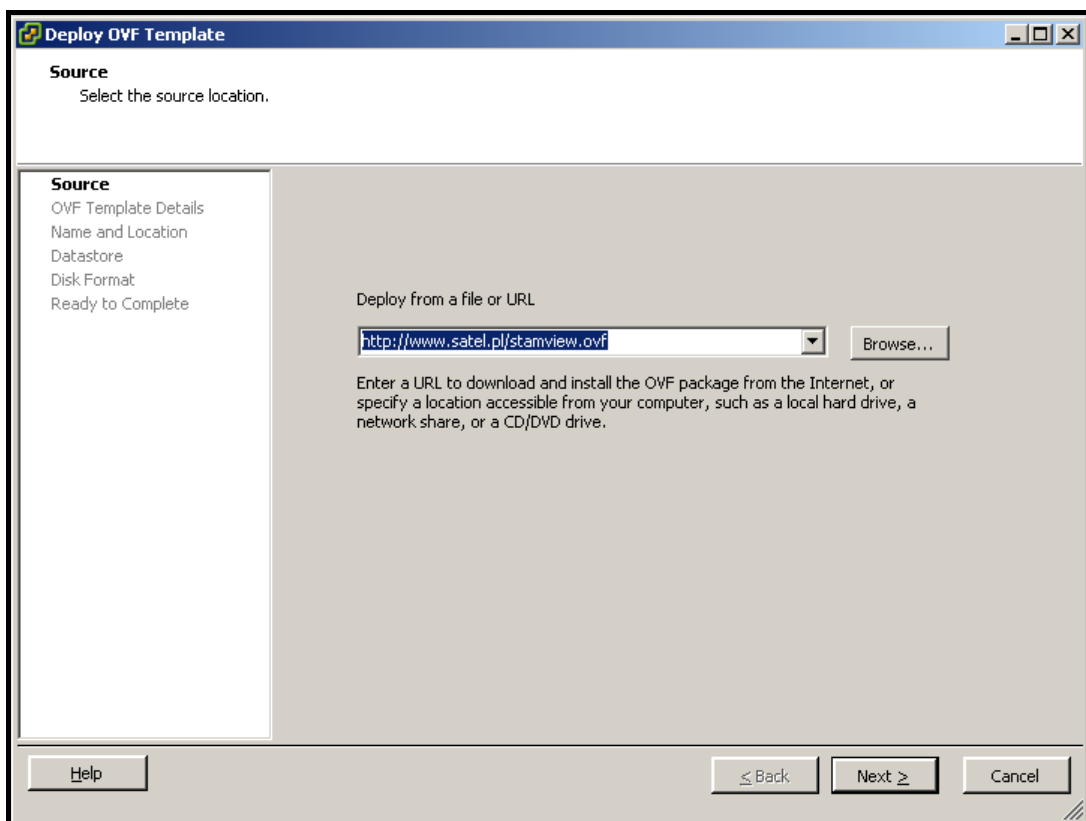
1. Open the web browser window and enter the IP address of VMware ESXi server. Once connected, click on the "Download vSphere Client" link to start installation of the program.
2. After the installation is complete, run the program by clicking on the program shortcut created on the desktop or in the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



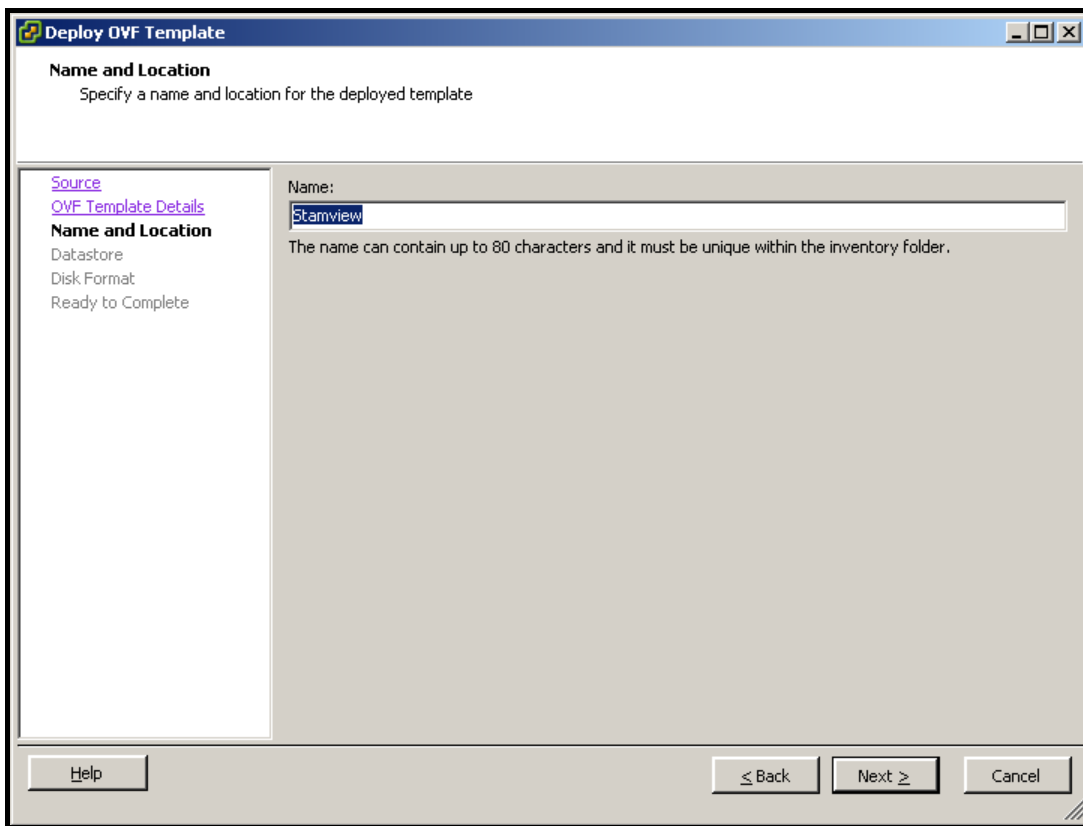
4. Select the "Deploy OVF Template" command in the "File" menu.



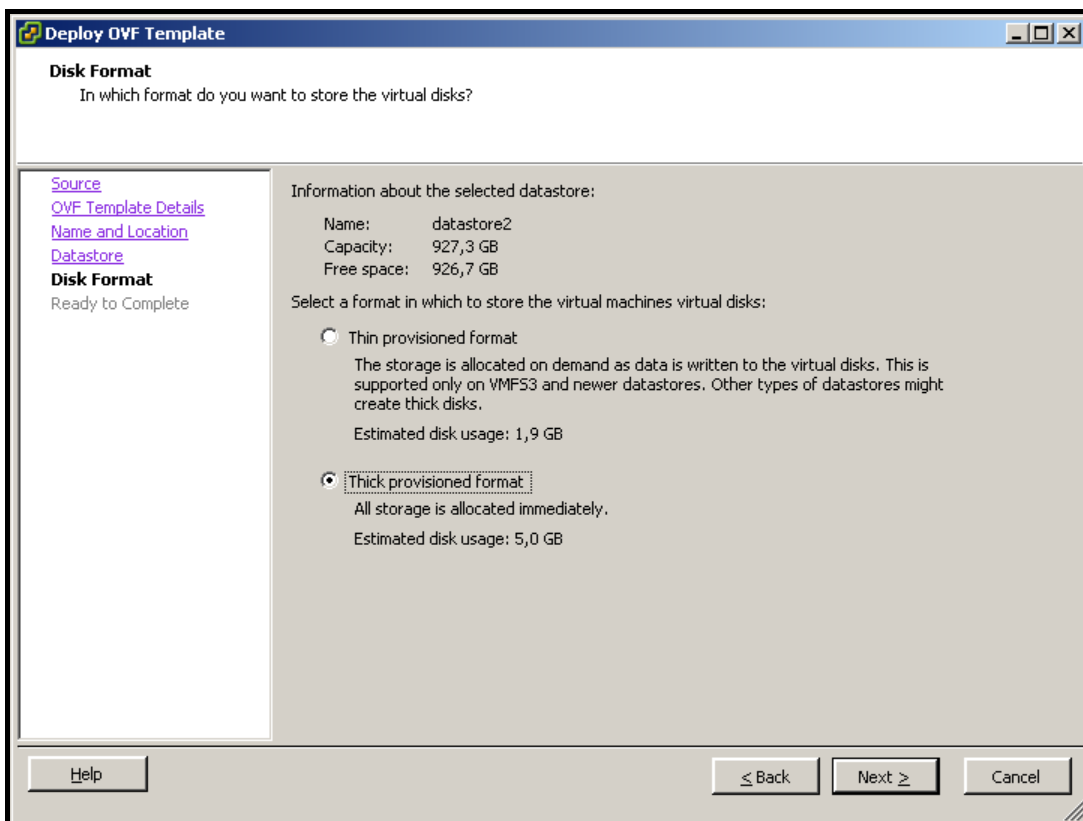
5. Enter the <http://www.satel.pl/stamview.ovf> address in the "Deploy from a file or URL" field and press NEXT.



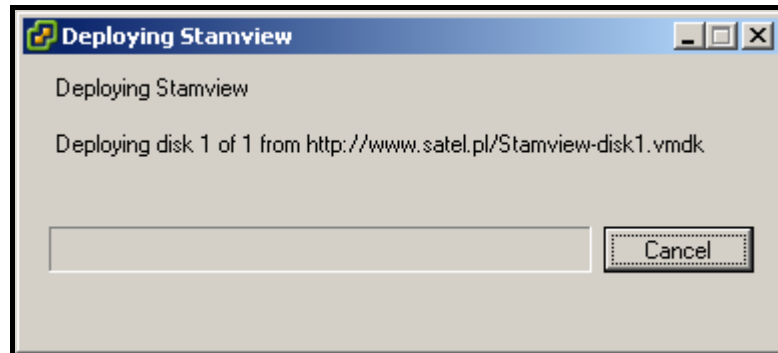
6. Enter the name of STAM-VIEW virtual machine and press NEXT.



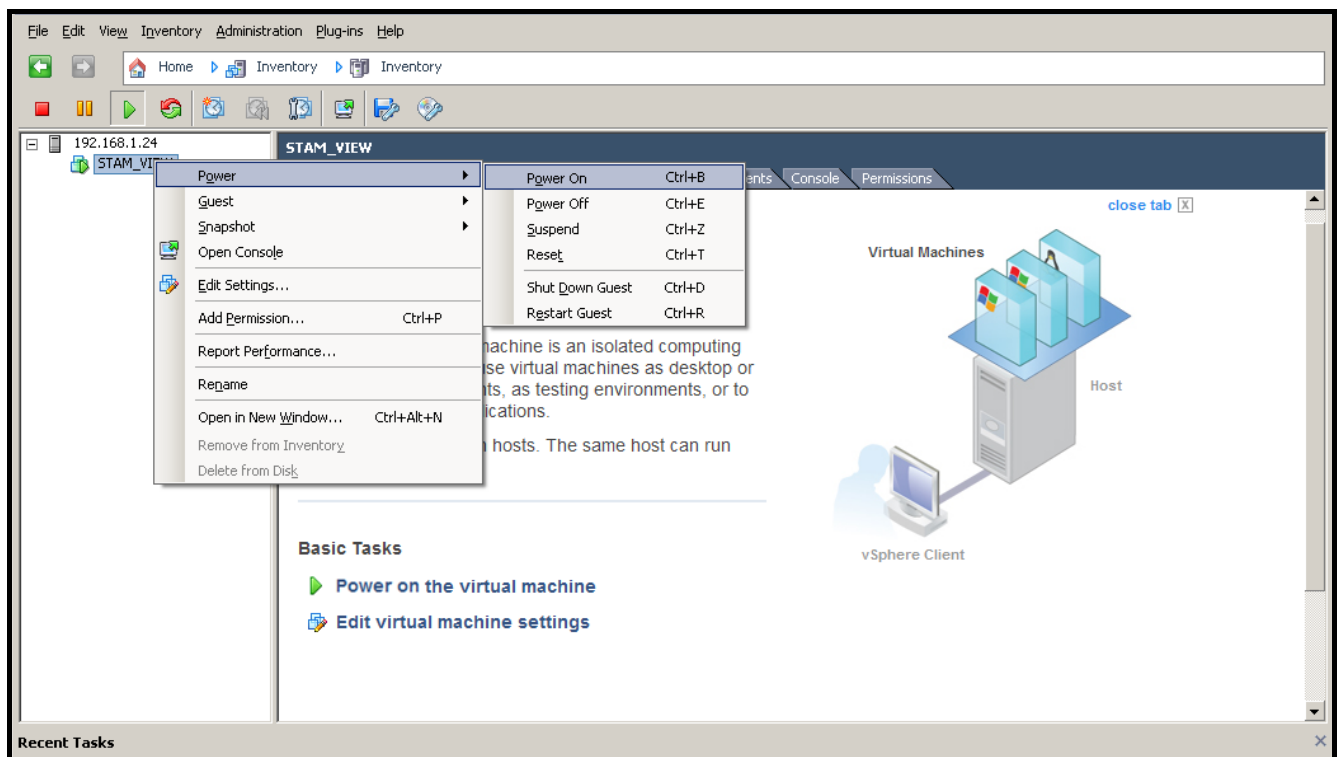
7. Select the disk on which the virtual machine is to be deployed and press NEXT.
8. Select the "Thick provisioned format" option and press NEXT.



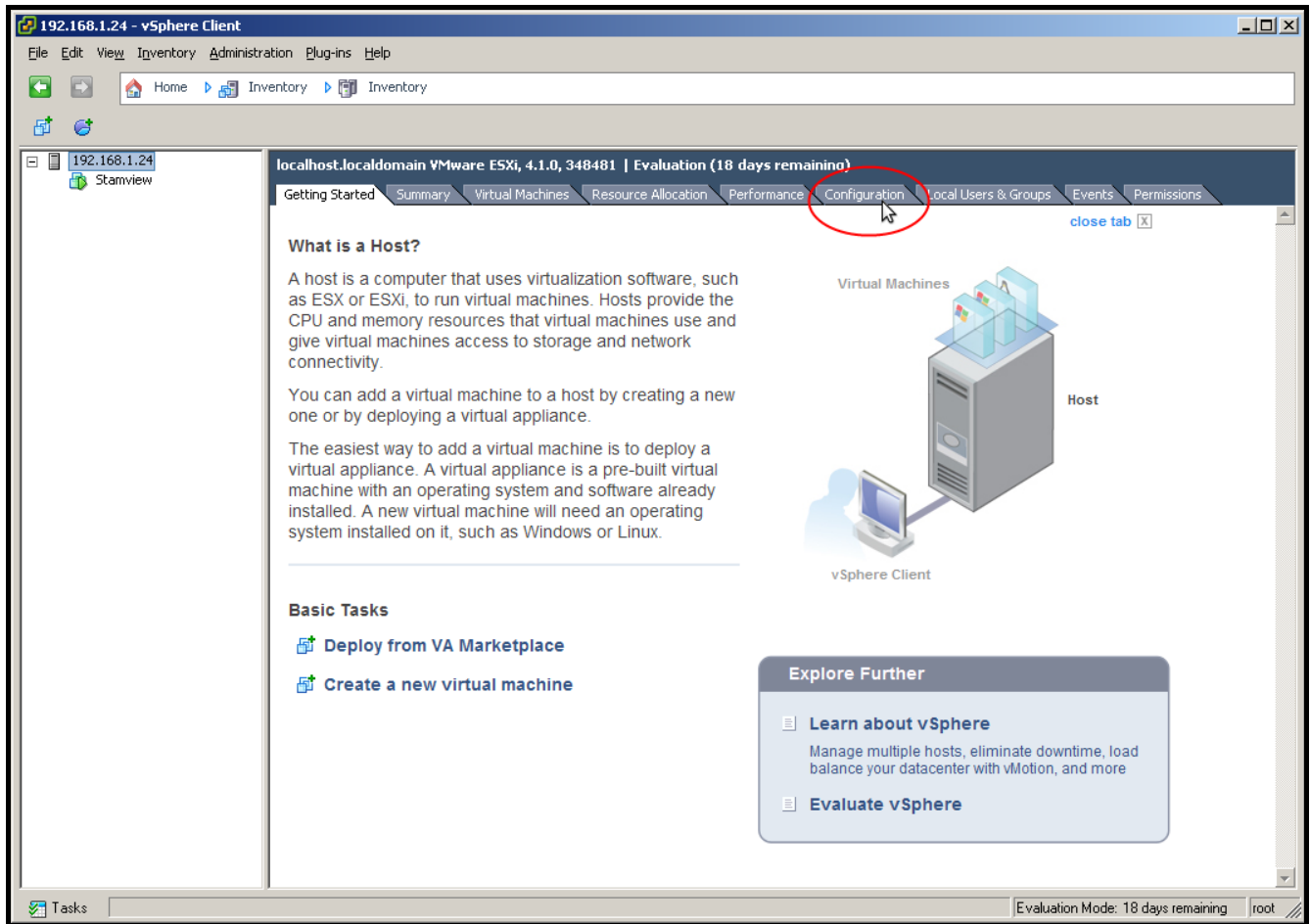
9. A summary of data on the virtual machine settings will be displayed. Press FINISH. The STAM-VIEW environment takes more than 530 MB, so the process of its importing may last up to about 1 hour.



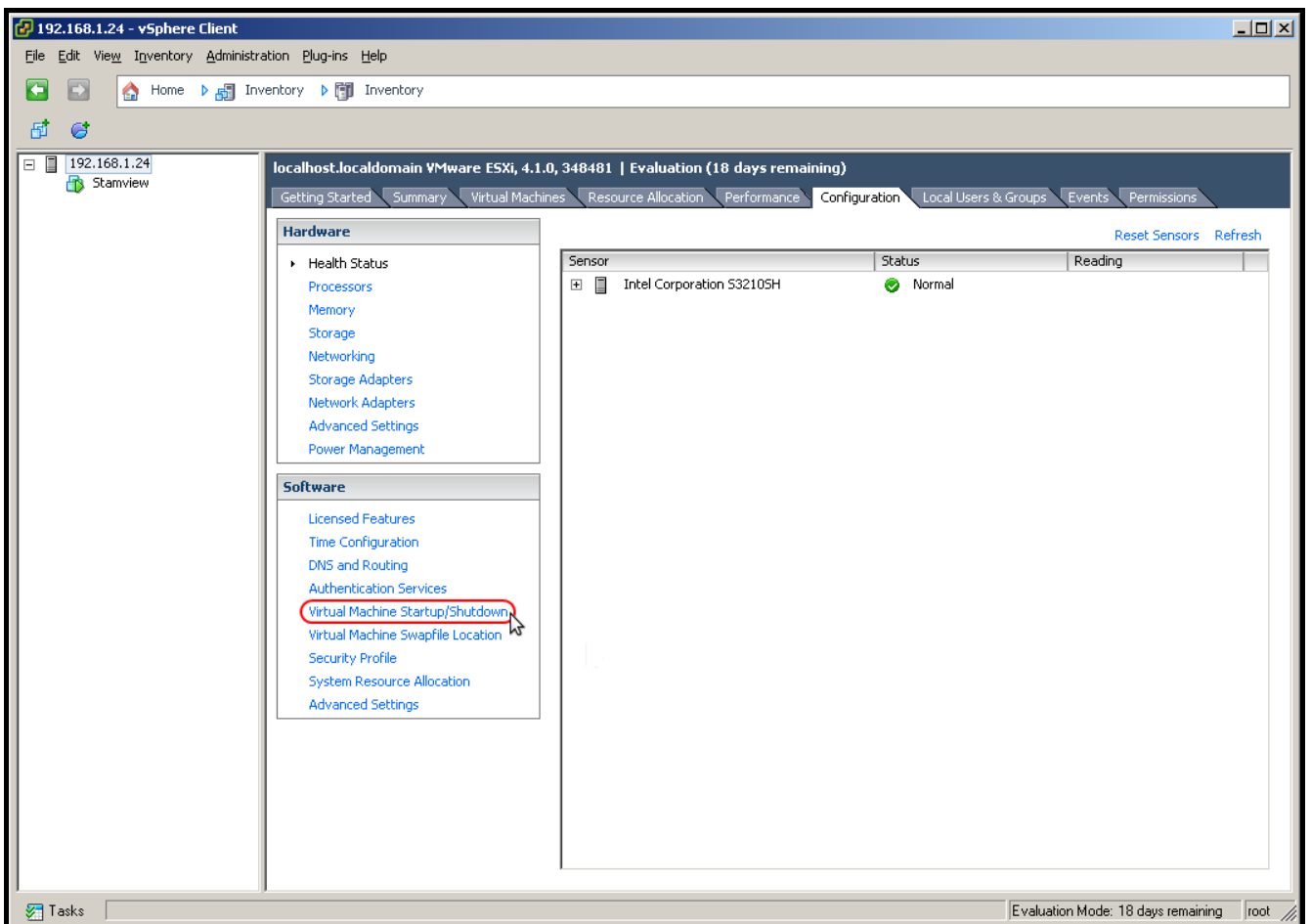
10. In order to run the imported machine, set the mouse cursor over the machine name and right-click. In the drop-down menu, click "Power" and then "Power On". The IP address of the machine with STAM-VIEW system installed, as shown in the screenshot, is just an example.



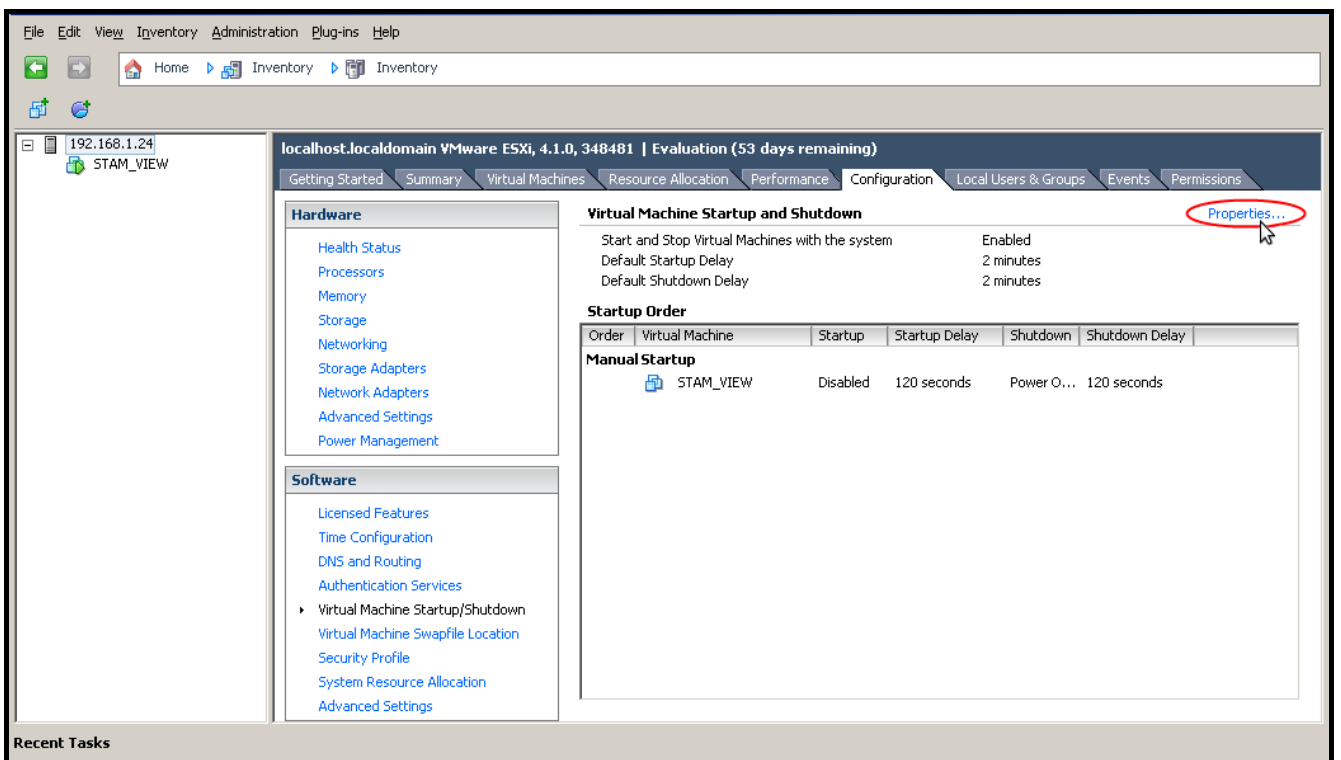
- 11. Turn the machine to run automatically. To do so, hover your mouse cursor over the machine address and left-click. You will see tabs with the server-related data. Select the "Configuration" tab.



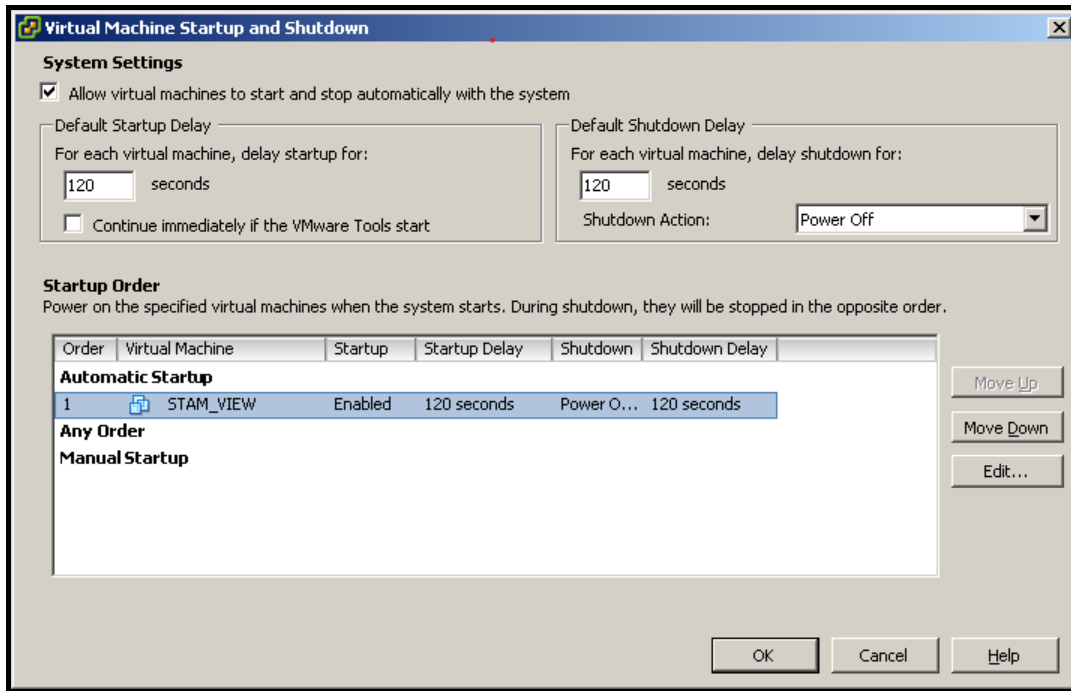
12. Click on "Virtual Machine Startup / Shutdown" in the "Software" area.



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.

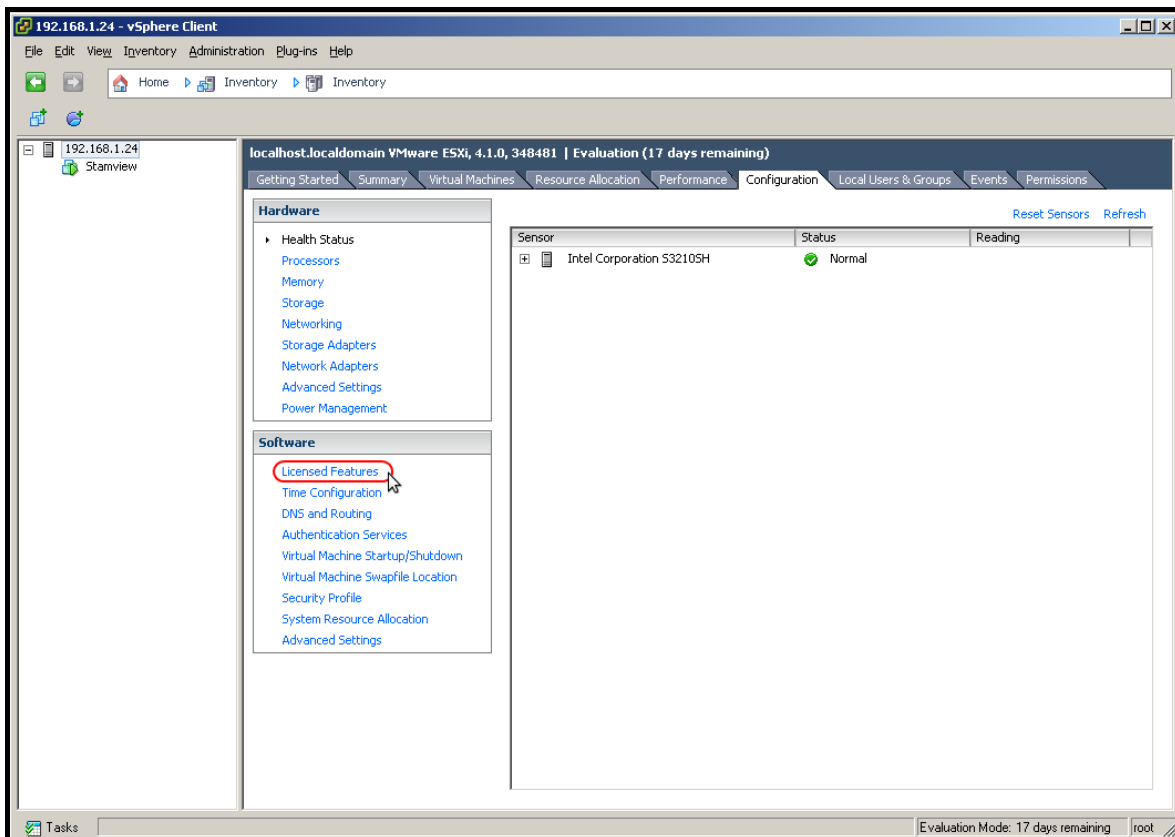


### 2.5.1 Entering license key

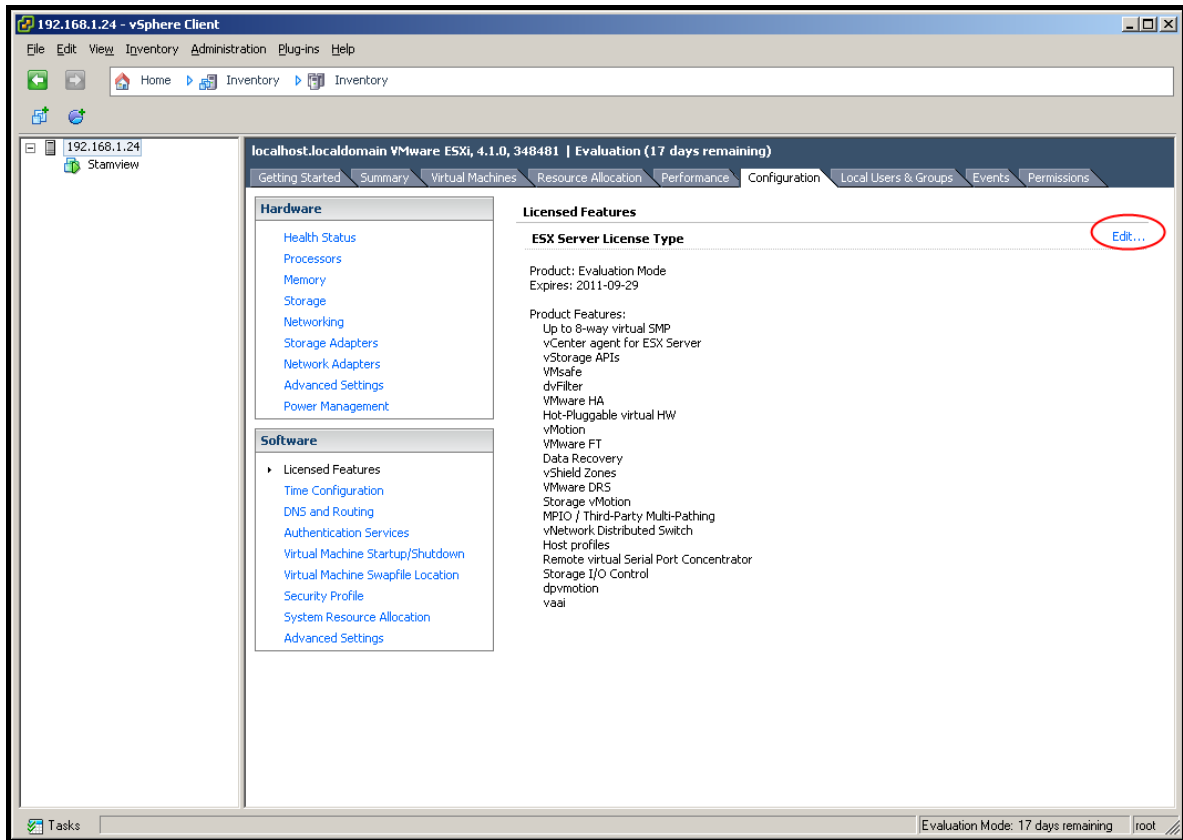


Be sure to enter the license key which is required for the proper operation of the program beyond the 60-day period. The key is available after you log in to your account on the site of the VMware software manufacturer.

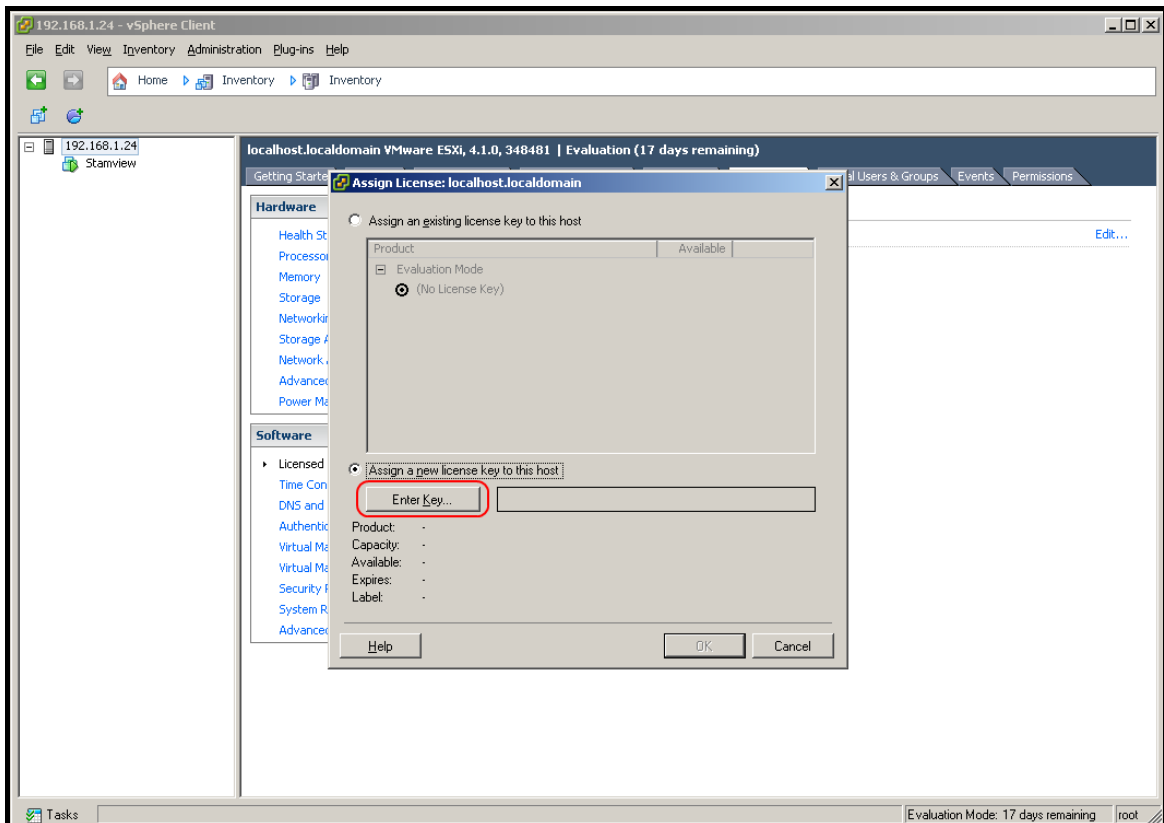
1. In the "Configuration" tab, click on the "Licensed Features" in the "Software" area.



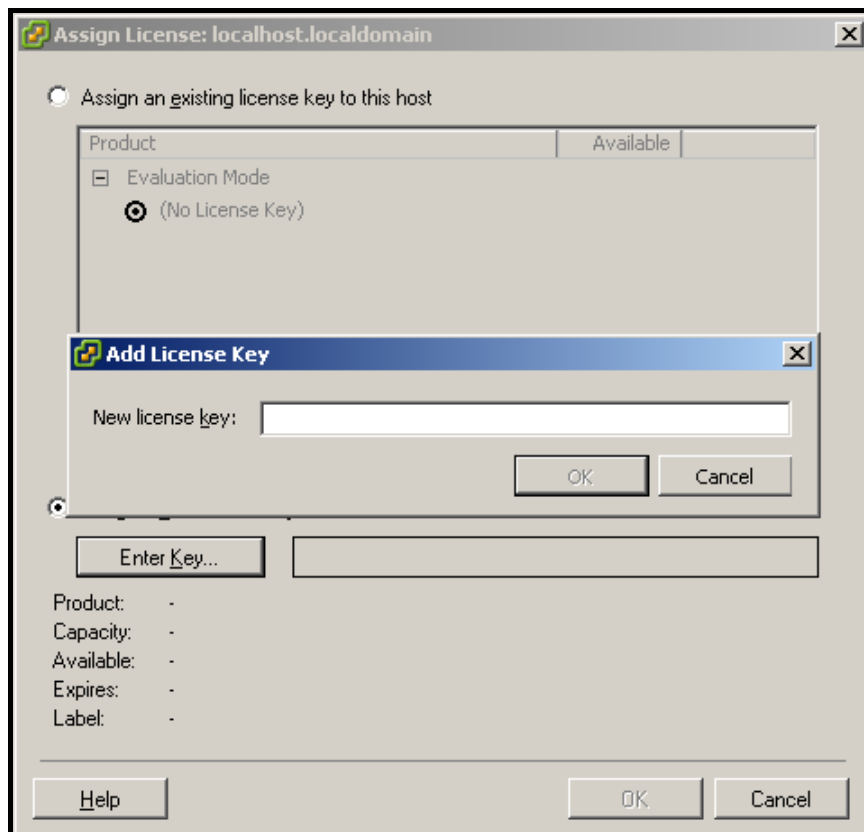
2. Select "Edit" in the upper right corner of the window.



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](http://www.startssl.com) address in your web browser.

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

**StartSSL™ - The Swiss Army Knife of Digital Certificates & PKI**

### Welcome to StartSSL™ PKI

StartSSL™ is the trade mark of the **StartCom Certification Authority** - a leader of the digital certification industry. We provide you with everything from **free** low-assurance **SSL** certificates up to the most advanced PKI and security solutions for your business and personal use.

- StartSSL™ Free (Class 1)**  
128/256-bit Encryption, **1 Year** Validity  
Legitimate SSL/TLS + S/MIME Certificates  
**No Charge, Unlimited + 100% Free**
- StartSSL™ Verified (Class 2)**  
128/256-bit Encryption, **2 Years** Validity  
Legitimate SSL/TLS + S/MIME + Object Code  
Wild Cards, Multiple Domain Names (UCC)  
**Unlimited Certificates - US\$ 59.90**
- StartSSL™ Extended Validation**  
128/256-bit Encryption, **2 Years** Validity  
Highest Level Third Party Assurance  
Green Extended Trust Indicator  
Multiple Domain Names (UCC)  
**Special Offer - US\$ 199.90**
- Hardware**  
Aladdin® USB eToken Pro  
Aladdin® Smart Cards + Reader  
Original Driver Software + PKI Client  
Enterprise PKI Customized Solutions
- Internationally Recognized**  
WebTrust for CAs + WebTrust EV Certified  
Recognized by major browsers + software vendors
- High Protection**  
StartSSL™ High Level Protection  
No MD5 Hashes, Weak Key Scans  
Minimum 2048-bit Strong RSA Keys
- Authentication**  
StartSSL™ Authentication SSL Protected  
Open Identity Authentication Provider  
Click here to log into your StartSSL™ Account
- Easy Enrollment**  
Sign-up and you will receive right away an S/MIME client-certificate and a digital StartSSL™ Open Identity without charge during the easy three-step enrollment!

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

**StartSSL™ - The Swiss Army Knife of Digital Certificates & PKI**

### StartSSL™ Free

The StartSSL™ Free (Class 1) digital certificates are provided by StartCom without charge. They provide modest assurances and are meant to secure personal web sites, public forums or web mail. Verification is done automatic and instantly by electronic means and mostly without the interference and involvement of our personnel. StartSSL™ Free supports:

- Web server certificates (SSL/TLS)
- Client and mail certificates (S/MIME)
- 128/256-bit encryption
- US \$ 10,000 insurance guaranteed
- Valid 365 days (1 year)

**...No Kidding 100% FREE**

For more information follow **this link** or **sign up** now for your StartSSL™ account and start to enjoy free digital certification immediately!

### StartSSL™ Verified

StartSSL™ Verified (Class 2) digital certificates are ideal for authentication, B2B and B2C transactions, protection of electronic mail and signing of object code and macros. More than that, StartSSL™ Verified provides a level of flexibility and support options not found anywhere else. StartSSL™ Verified supports:

- Web server certificates (SSL/TLS)
- Wild cards (\*.domain.com)
- Multiple domains (DNS Alt Names)
- 128/256-bit encryption
- Object Code Signing
- Client and mail certificates (S/MIME)
- US \$ 10,000 insurance guaranteed
- Certificates **2 Years** valid (730 days)

**Wildcard & Multiple Domains Unlimited Certificates, only US\$ 59.90**

Make sure to read the **requirements** and **enroll** for StartSSL™ Verified.

### StartSSL™ Extended Validation

StartSSL™ Extended Validation certificates help to increase identity awareness and customer confidence due to the the new


### StartSSL™ Web-of-Trust

The StartSSL™ Web-of-Trust (WoT) is an attempt by StartCom to create a community network of StartSSL™ appointed notaries and members.


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

### Authenticate or Sign-up?


**Are you a returning subscriber?** Or do you want to authenticate with your StartSSL™ Open Identity?  
Please click the button below and choose your StartSSL™ certificate from the dialog.



**Are you the first time here?** Sign up and receive right away an email certificate (S/MIME) and a digital StartSSL™ Open Identity without charge during the easy three-step enrollment!



**...or get a StartSSL™ Free server certificate real quick!**  
Follow the Express Lane which will guide you through all the necessary steps. Choose this option only if this is your first time here, otherwise log into your account above.



- You must enable JavaScript and cookies support at your browser since this site will not work without it.
- The email certificate (S/MIME) can be used for the signing and encryption of your electronic mail. The certificate will be installed into your browser, just backup and import it into your favorite mail client for this purpose.

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

#### Personal Enrollment Details:

- All fields are required!** You must provide your correct and complete **personal details** during initial registration! Be advised, that we may **check and verify the validity** of the information submitted. Misleading and wrong information will result in the blocking of access and revocation of certificates! See also **this FAQ entry** for more information.
- Privacy:** The personal details may be used in part or in full in certificates or digital identities. They may be presented in a summarized form to potential investors and business partners, but not in details. We refrain from contacting you, except in cases relevant for the service we provide or for clarifications. We will not distribute your details to any third party, except if ordered to do so by law.
- By using this service you confirm, that you have read the **CA Policy** and accept the terms and conditions outlined in this document. Only a **natural person** can enter into the subscriber agreement during initial registration.

**Important: Read and follow all instructions carefully! You are required to adhere to our terms and conditions!**

First, Last Name:   ⓘ

Complete Home Address (Street, House, Number):  ⓘ

Zip, Locality/Place:  ,  ⓘ

Country:  ▾

State/Region \*\*:  ▾

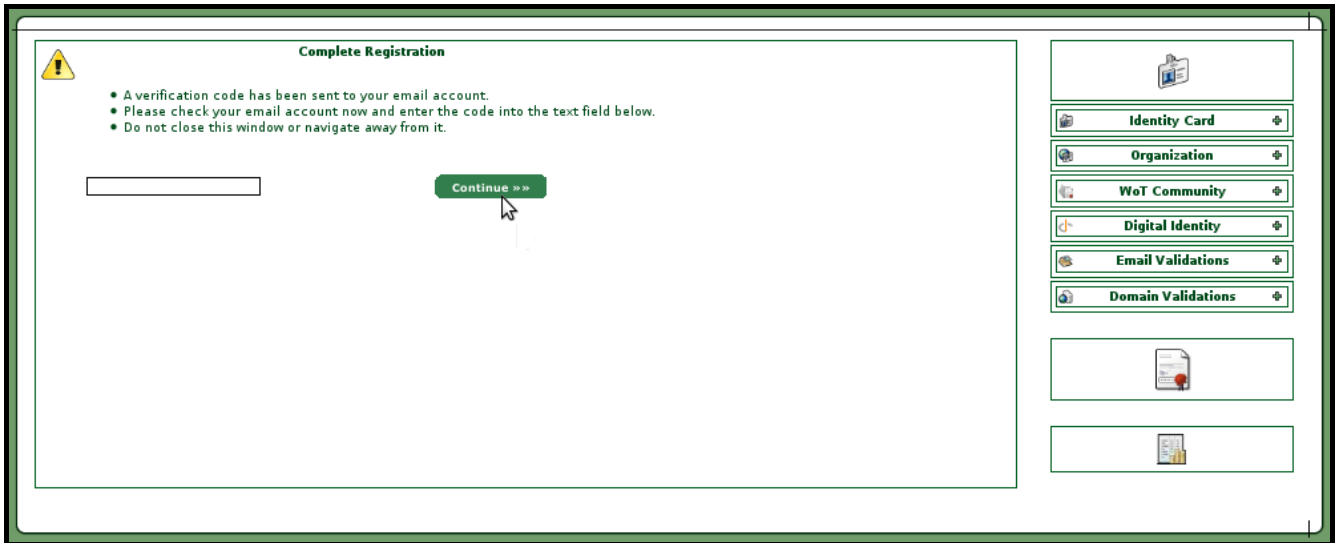
Phone:  ⓘ

Email \*:  ⓘ

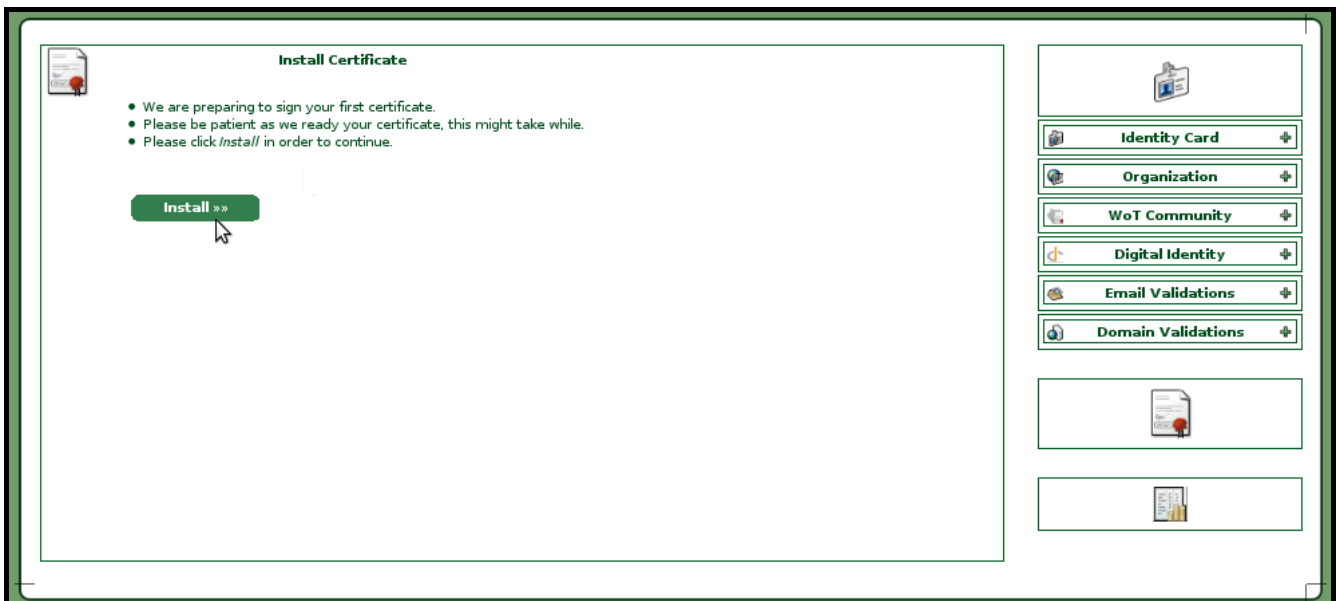
\* Mail accounts from the following providers are not allowed: qq.com freemail.com rambler.ru mailnull.com laposte.fr yopmail.com  
 \*\* Not seeing the States/Regions? Make sure you have JavaScript enabled.  
 \*\*\* States/Regions still missing of your country? Please help to improve it! **Send** a complete list to us.

**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](http://www.startssl.com) page.
9. Click the "Install" button to install the personal certificate.



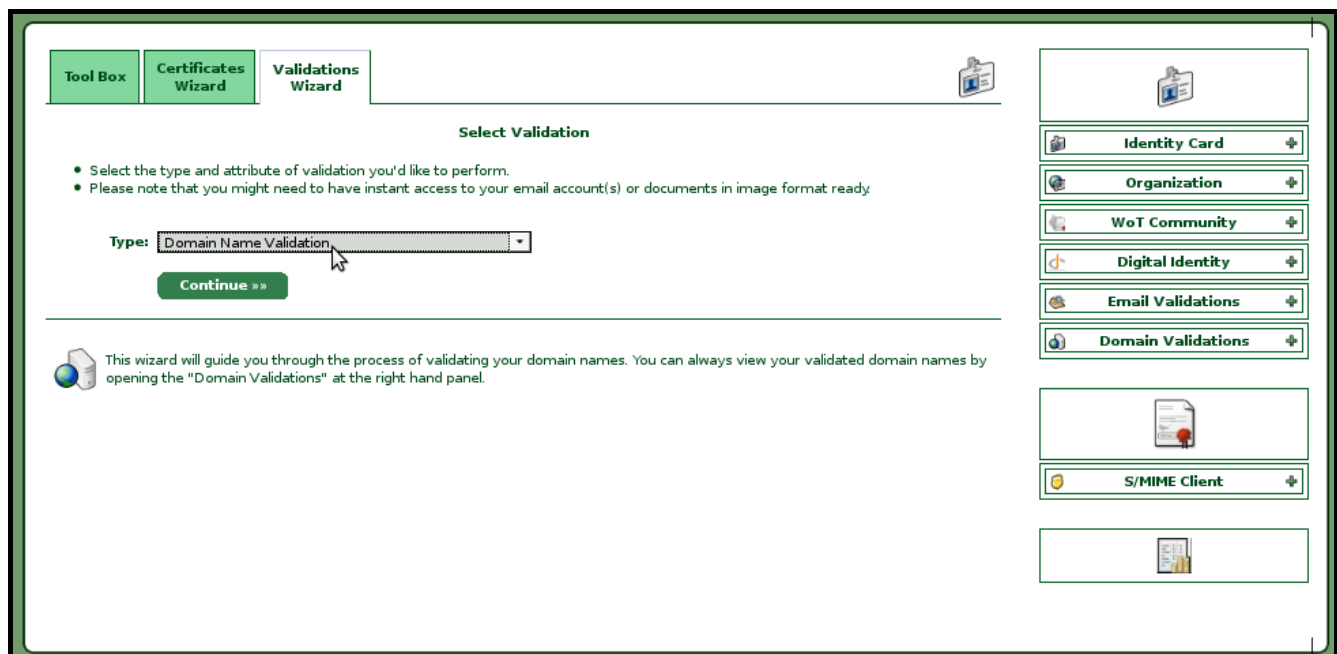
10. The certificate will be permanently installed in your web browser. It is recommended that you keep a backup copy of it (to do so, see the "How do I backup my client certificates?" instructions in the "F. A. Q." tab at the <http://www.startssl.com/?app=25> web page). Click "Finish".

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.



The screenshot shows the StartSSL Control Panel interface. At the top, there are three tabs: "Tool Box", "Certificates Wizard", and "Validations Wizard", with the latter being the active tab. A mouse cursor is pointing at the "Validations Wizard" tab. Below the tabs, a welcome message reads: "Howdy Jan Kowalski! Welcome to your StartSSL™ Control Panel...". A paragraph of text explains the benefits of validation for Class 2 and EV level certificates. Under the heading "Getting Started:", there are three numbered steps: 1. Validate, 2. Certificate, and 3. Various. On the right side of the panel, there is a vertical list of menu items: Identity Card, Organization, WoT Community, Digital Identity, Email Validations, Domain Validations, S/MIME Client, and another item partially visible at the bottom.

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



The screenshot shows the "Select Validation" step in the StartSSL Control Panel. The "Validations Wizard" tab is still active. The main content area has the heading "Select Validation" and two bullet points: "Select the type and attribute of validation you'd like to perform." and "Please note that you might need to have instant access to your email account(s) or documents in image format ready." Below this, there is a "Type:" label followed by a dropdown menu where "Domain Name Validation" is selected. A "Continue »»" button is positioned below the dropdown. At the bottom left, there is a small globe icon and a paragraph of text: "This wizard will guide you through the process of validating your domain names. You can always view your validated domain names by opening the 'Domain Validations' at the right hand panel." The right-hand menu is identical to the previous screenshot.

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

The screenshot shows the 'Enter Domain Name' step of the SATEL installation wizard. The interface includes a top navigation bar with 'Tool Box', 'Certificates Wizard', and 'Validations Wizard'. The main content area is titled 'Enter Domain Name' and contains the following instructions:

- Enter the domain name you want to have validated.
- You must be the owner of the top-level domain, sub domains are not supported.

The domain name input field is pre-filled with 'http://stamview.pl'. A 'Continue >>' button is located below the input field. On the right side of the screen, there is a vertical sidebar with several expandable menu items: Identity Card, Organization, WoT Community, Digital Identity, Email Validations, Domain Validations, S/MIME Client, and another item partially visible at the bottom.

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".

The screenshot shows the 'Select Verification Email' step of the SATEL installation wizard. The interface includes a top navigation bar with 'Tool Box', 'Certificates Wizard', and 'Validations Wizard'. The main content area is titled 'Select Verification Email' and contains the following instruction:

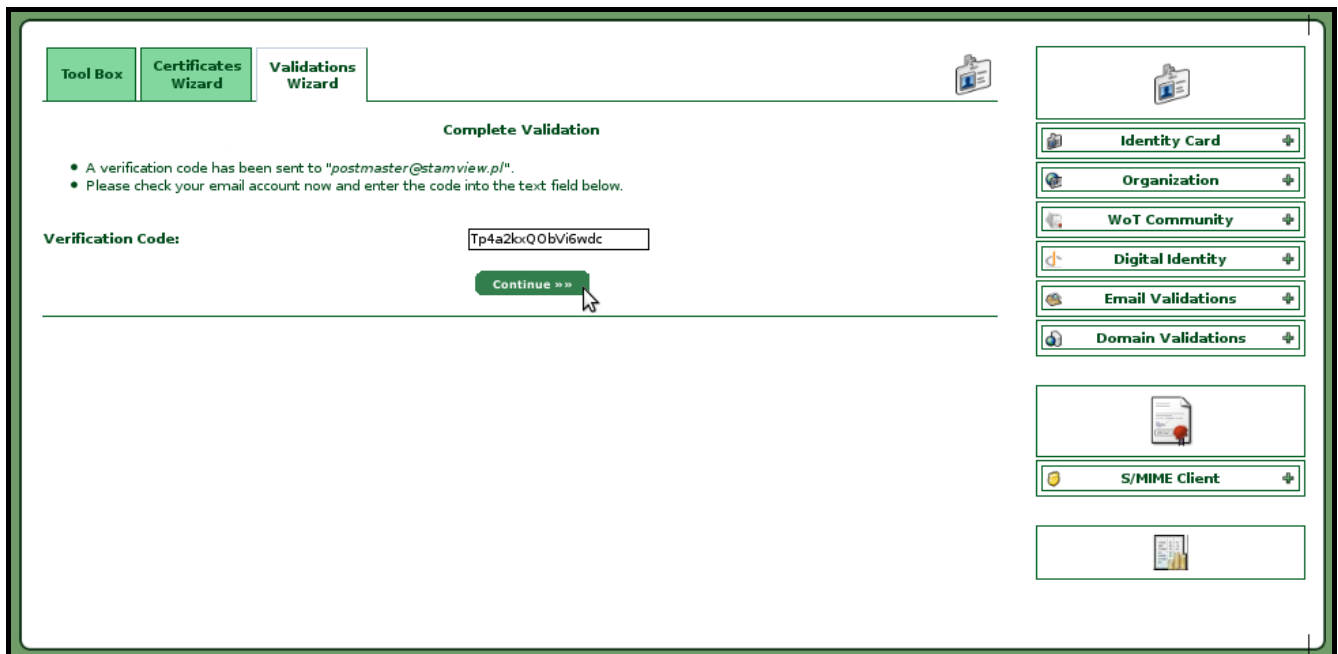
- Select the email address for verification of domain ownership from below.

The 'Verification Email:' section lists four options with radio buttons:

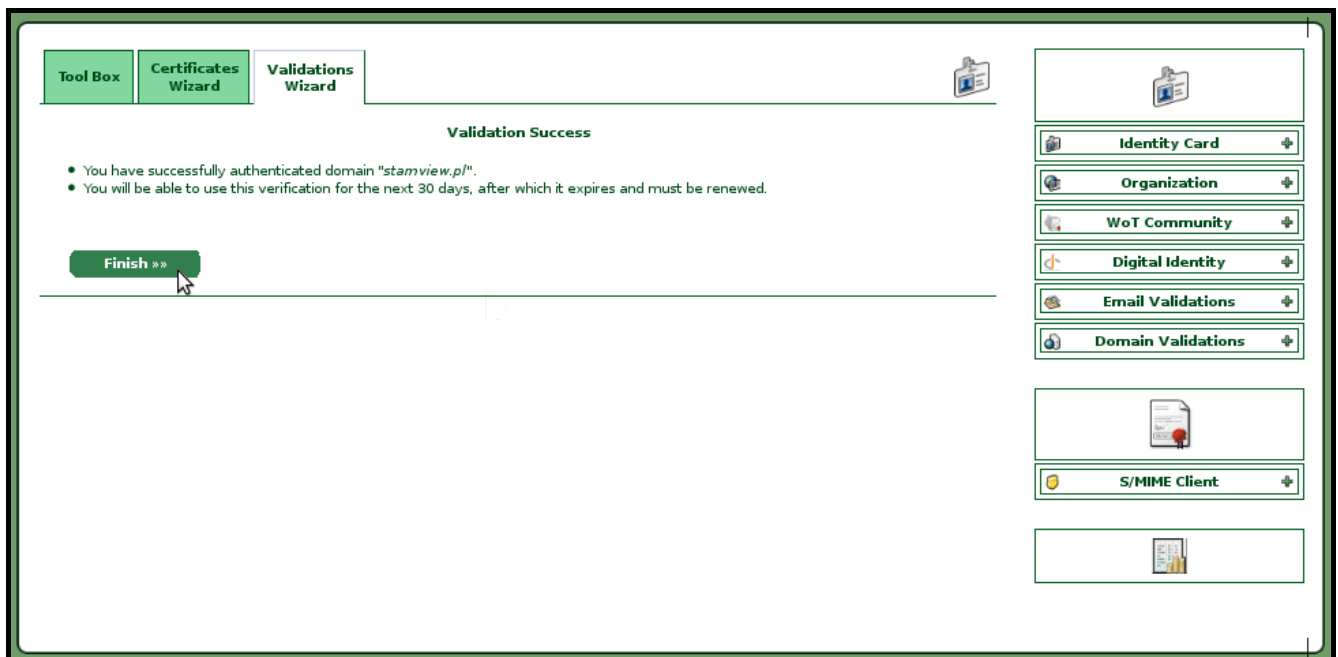
- postmaster@stamview.pl
- hostmaster@stamview.pl
- webmaster@stamview.pl
- domeny@consultingservice.pl

A 'Continue >>' button is located below the list, with a mouse cursor pointing to it. On the right side of the screen, there is a vertical sidebar with several expandable menu items: Identity Card, Organization, WoT Community, Digital Identity, Email Validations, Domain Validations, S/MIME Client, and another item partially visible at the bottom.

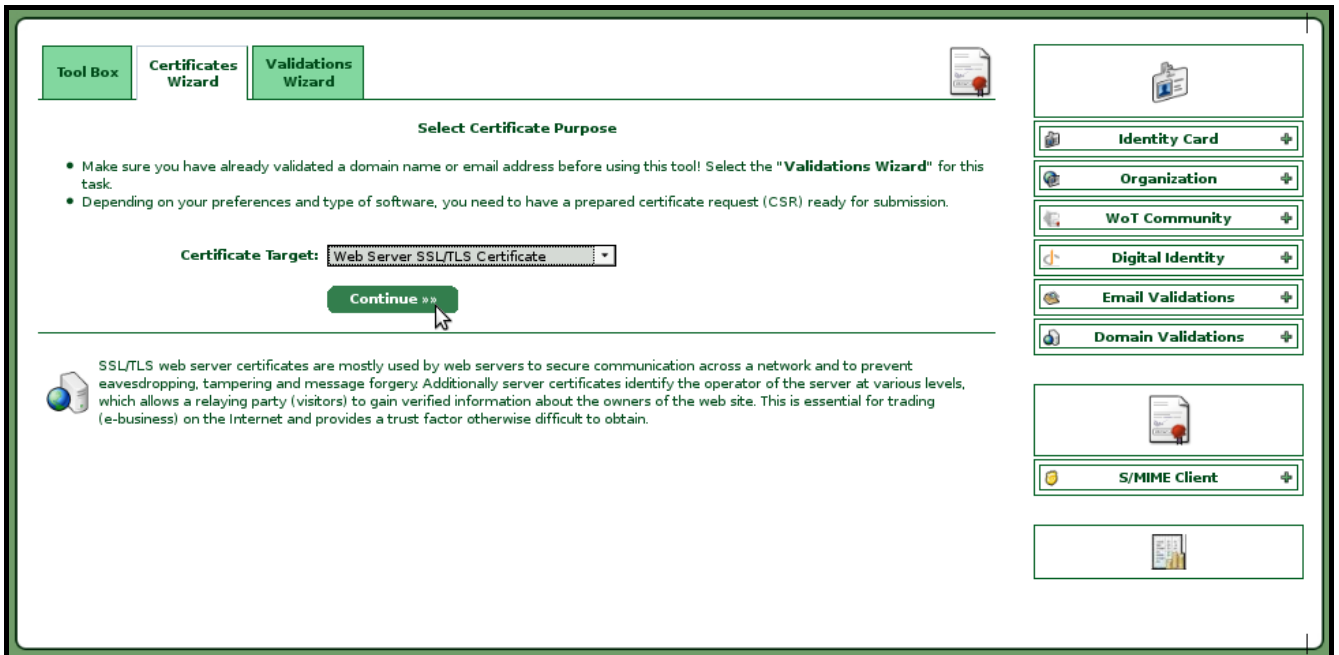
15. In the "Verification Code", enter the code you received in the email message sent to the address indicated in the previous window. Click "Continue".



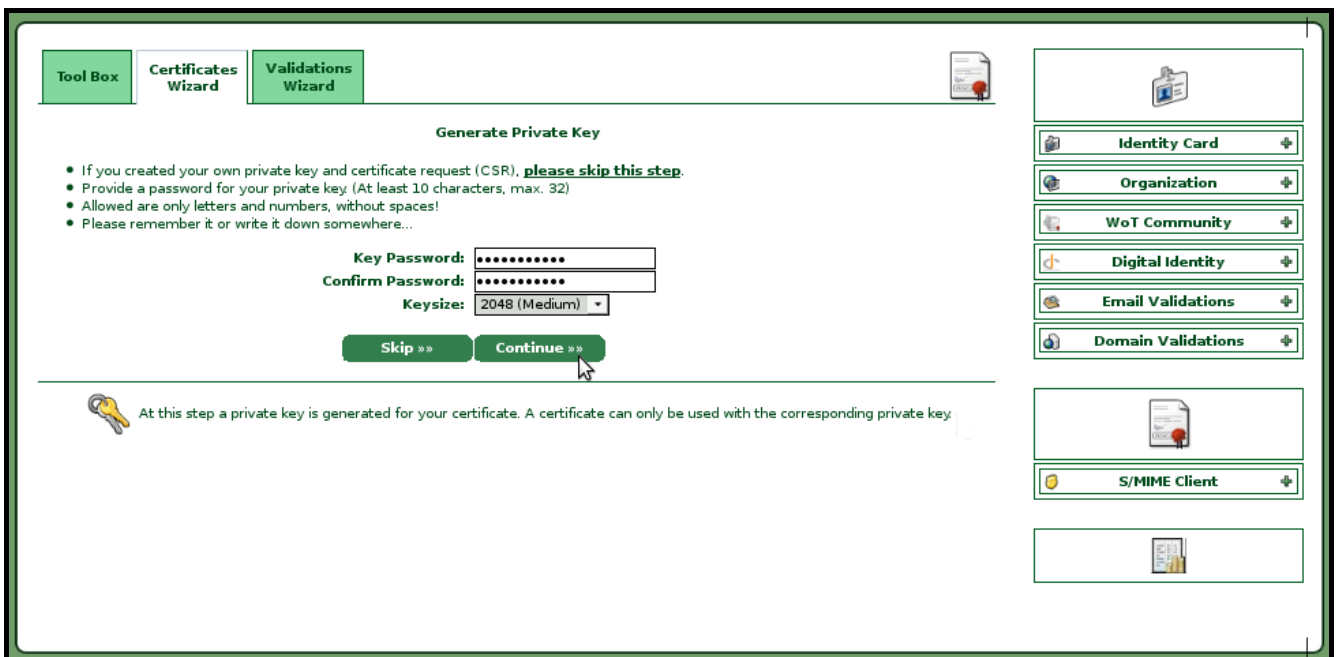
16. Click on the "Finish" button.



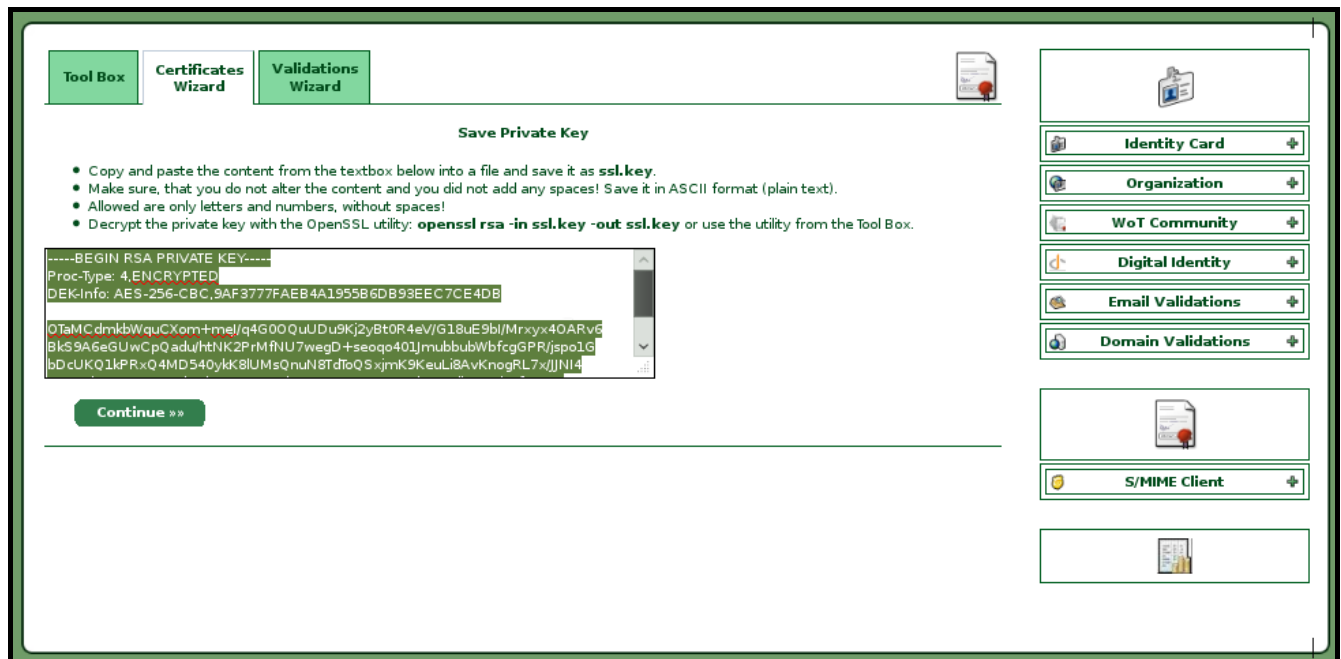
17. Click on the "Certificates Wizard" tab. In the "Certificate Target" field, select the "Web Server SSL/TLS Certificate" option and click "Continue".



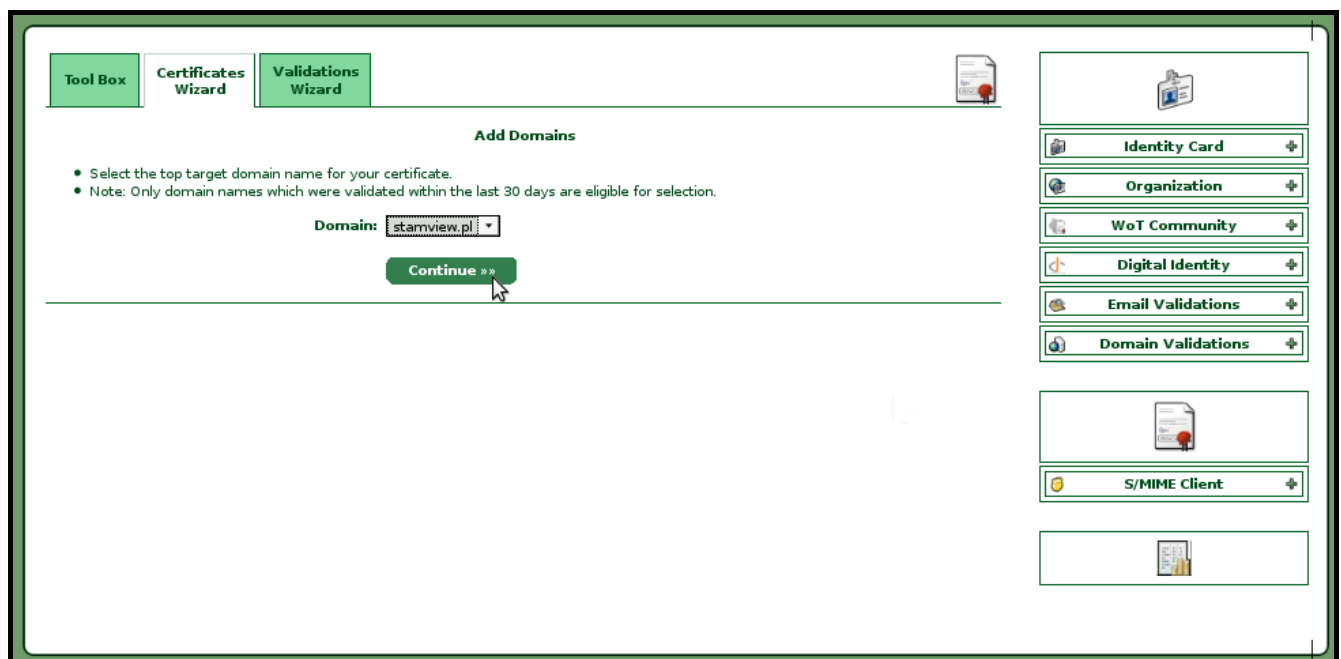
18. Enter your password in the "Key password" field. You can enter from 10 to 32 characters (digits and letters). To confirm the password, type it again in the "Confirm Password" field. Click "Continue".



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".



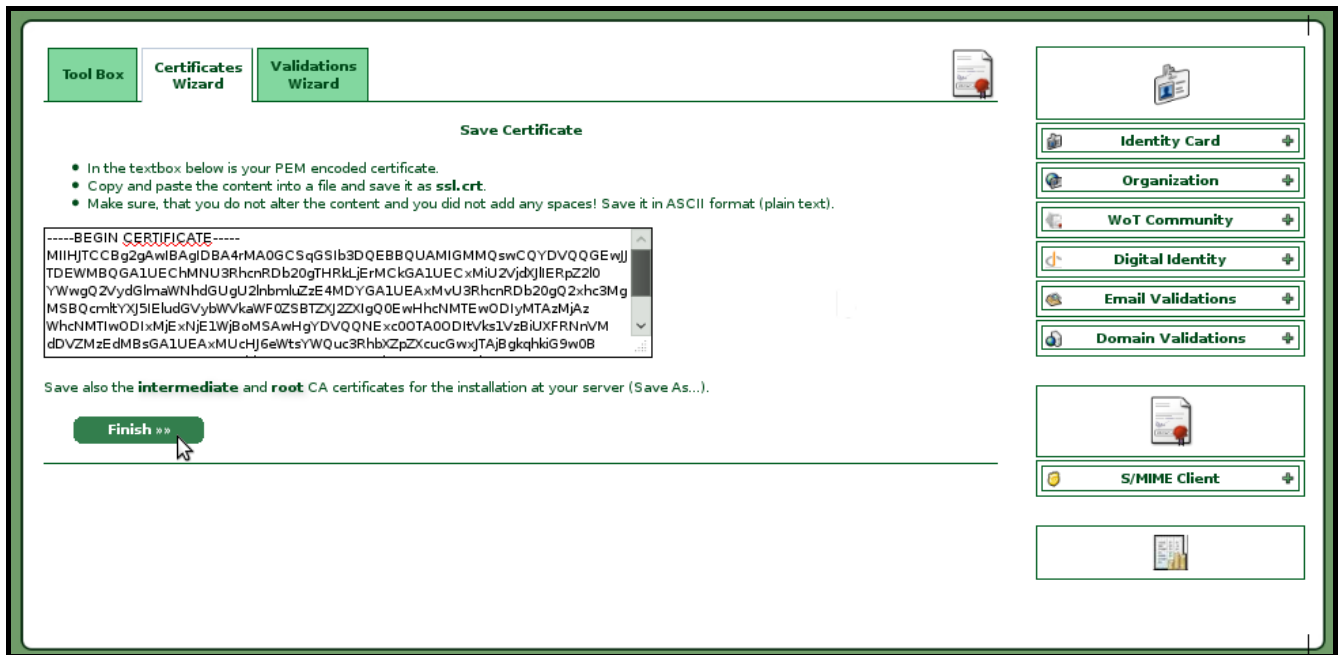
21. Create a subdomain under the previously verified domain. This will be an address of the STAM-VIEW system to which the users will log in. Given in the window below is a sample address: `http://przyklad.stamview.pl`. Click "Continue".

The screenshot shows the 'Add Domains' step of the Certificates Wizard. The interface includes a 'Tool Box' with 'Certificates Wizard' and 'Validations Wizard' tabs. A list of instructions is provided: 'You must add one sub domain to this certificate.', 'The base domain `stamview.pl` will be included by default in the Alt Name section.', and 'Note: In order to add multiple domains and sub domains, your Identity must be at least **Class 2** validated. Check your status at the "Identity Card".'. A text input field contains the URL `http://przyklad.stamview.pl`. A green 'Continue >>' button is visible below the input field. On the right side, there are several expandable menu items: 'Identity Card', 'Organization', 'WoT Community', 'Digital Identity', 'Email Validations', 'Domain Validations', 'S/MIME Client', and another empty item.

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

The screenshot shows the 'Ready Processing Certificate' step of the Certificates Wizard. The interface includes the same 'Tool Box' with 'Certificates Wizard' and 'Validations Wizard' tabs. A list of instructions is provided: 'We have gathered enough information in order to sign your certificate now.', 'The common name of this certificate will be set to `przyklad.stamview.pl`.', 'The certificate will have the following host names supported: 1. `stamview.pl`, 2. `przyklad.stamview.pl`', and 'Please click on *Continue* in order to process the certificate.'. A green 'Continue >>' button is visible below the instructions. On the right side, there are several expandable menu items: 'Identity Card', 'Organization', 'WoT Community', 'Digital Identity', 'Email Validations', 'Domain Validations', 'S/MIME Client', and another empty item.

- 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 encrypted. 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.

Welcome in remote access system for STAM-2 monitoring station EN PL SK

Login:

Password:

  
Click on picture, if it's unreadable

Security code:

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".

The screenshot shows the Satel Stam-View web interface. The top header includes the Satel logo, the title "Stam-View - remote access system for STAM-2 monitoring station", the date and time "16-01-2012 13:02", and the language "EN PL RU". A "Log out" button is visible in the top right. The left sidebar contains navigation options: "Add user", "Show users", "Event log", "Messages", "Settings" (highlighted), "Logs", "Backup copy", and "Update". The main content area shows a welcome message for the Administrator and the last login details. The "Settings" section is active, with the "SSL Certificates" tab selected. It displays the current status of SSL certificates and provides options to upload new ones.

**Settings**

Welcome, **Administrator** **Last log in:** 2012-01-16 12:54:36, **Failed:** 2012-01-12 08:42:42

16-01-2012 13:02 EN PL RU

9:52 **Log out**

Add user  
Show users  
Event log  
Messages  
**Settings**  
Logs  
Backup copy  
Update

Settings

Password Logo Users Installers **SSL Certificates** Languages

**SSL certificates status**

Certificate file (\*.cert): Default (change required)

Key file (\*.key): Default (change required)

**Certification authority files**

CA file: StartSSL

Certificate chain file: StartSSL

**Upload certificates**

Certificate file (\*.cert):  Browse\_

Key file (\*.key):  Browse\_

Key password (if encoded):

**Upload**

**Upload certificates**

CA file:  Browse\_

Certificate chain file:  Browse\_

**Upload**

## 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

The screenshot shows the Stam-View remote access system interface. The header includes the Satel logo, the system name "Stam-View - remote access system for STAM-2 monitoring station", the date and time "16-01-2012 13:22", and language options "EN PL RU". A "Log out" button is visible in the top right corner. The main content area displays a welcome message, unread messages count (0), events since last entry (0), and a status table. The status table shows "Stam-View version" as OK, "Registered in STAM-2" as OK, and "SSL Certificates" as Check. Below the status table, the version information is displayed as "Version 28102011 (BETA)".

Status	
Stam-View version	OK
Registered in STAM-2	OK
SSL Certificates	Check

Version	
Version	28102011 (BETA)

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](http://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:

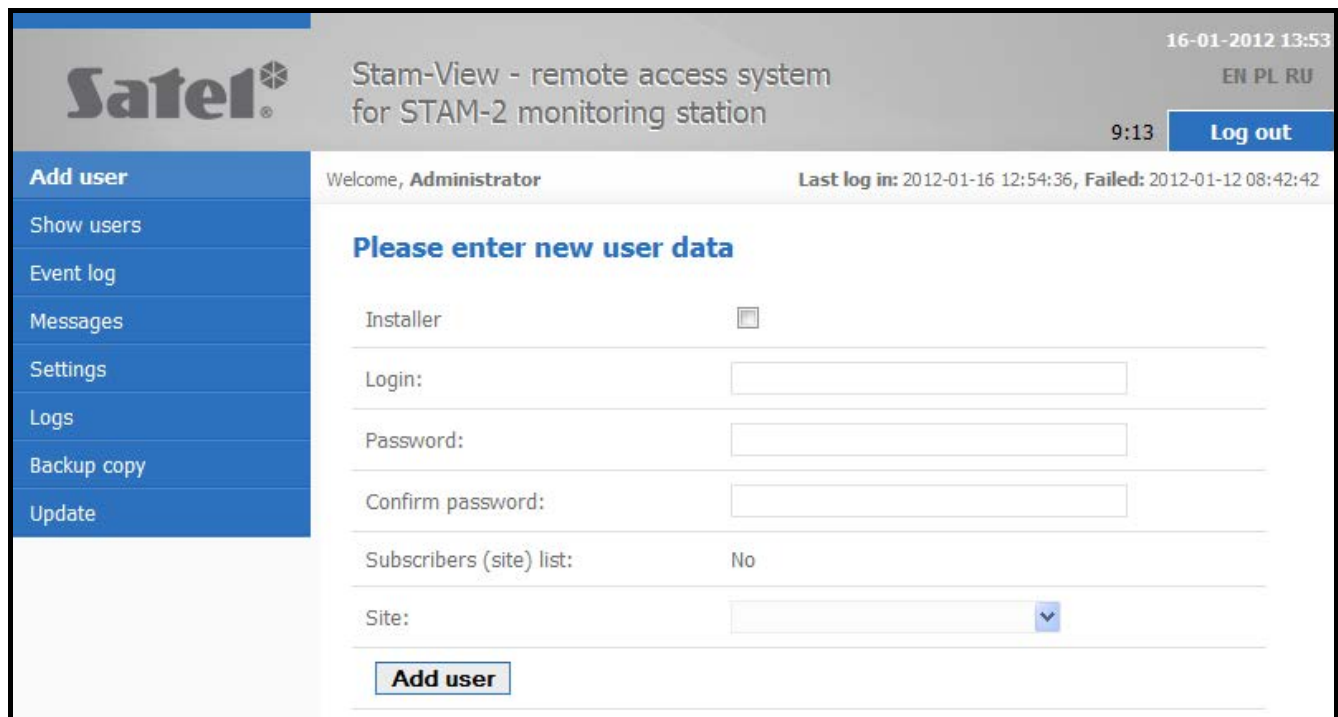
1. Log in to the system.
2. Enter the "Settings" tab and then the "Logo" tab in it.
3. Click the "Browse" button and select the file with preselected logo.

**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.



The screenshot displays the administrator interface for the Stam-View system. The top header includes the Satel logo, the system name 'Stam-View - remote access system for STAM-2 monitoring station', the date and time '16-01-2012 13:53', and language options 'EN PL RU'. A 'Log out' button is visible in the top right. The left sidebar contains a menu with options: 'Add user', 'Show users', 'Event log', 'Messages', 'Settings', 'Logs', 'Backup copy', and 'Update'. The main content area shows a 'Welcome, Administrator' message and a 'Last log in' status. The primary section is titled 'Please enter new user data' and contains the following form fields:

- Installer:** A checkbox.
- Login:** A text input field.
- Password:** A text input field.
- Confirm password:** A text input field.
- Subscribers (site) list:** A dropdown menu currently set to 'No'.
- Site:** A dropdown menu.

An 'Add user' button is located at the bottom of the form.


3. Ability to search for users by their name.

The screenshot displays the SATEL Stam-View web interface. At the top left is the SATEL logo. The main header area contains the text "Stam-View - remote access system for STAM-2 monitoring station" and the date "16-01-2012 14:19". A "Log out" button is visible in the top right. A navigation sidebar on the left lists options: "Add user", "Show users", "Event log", "Messages", "Settings", "Logs", "Backup copy", and "Update". The main content area shows a "Registered users" section with a search input field and a "Search for user" button. Below this is a table of users with columns for "User", "User type", and "Actions".

User	User type	Actions
Administrator	Administrator	
Armstrong_F	User	
Browning_W	User	
Brown_P	Installer	
Caine_R	User	
Cameron_C	Installer	
Carmichael_L	User	
Carnegie_E	User	
Cimino_D	User	
Derek_O	User	

At the bottom of the user list, there is a pagination control showing "page 1 from 3" and "next >>" along with a "Results per page" dropdown menu set to "10".

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.



Stam-View - remote access system  
for STAM-2 monitoring station

07-02-2012 09:18  
EN PL RU

Welcome, **Administrator**

8:46 Log out

Add user

Show users

**Event log**

Messages

Settings


Logs

Backup copy

Update

**Events log**

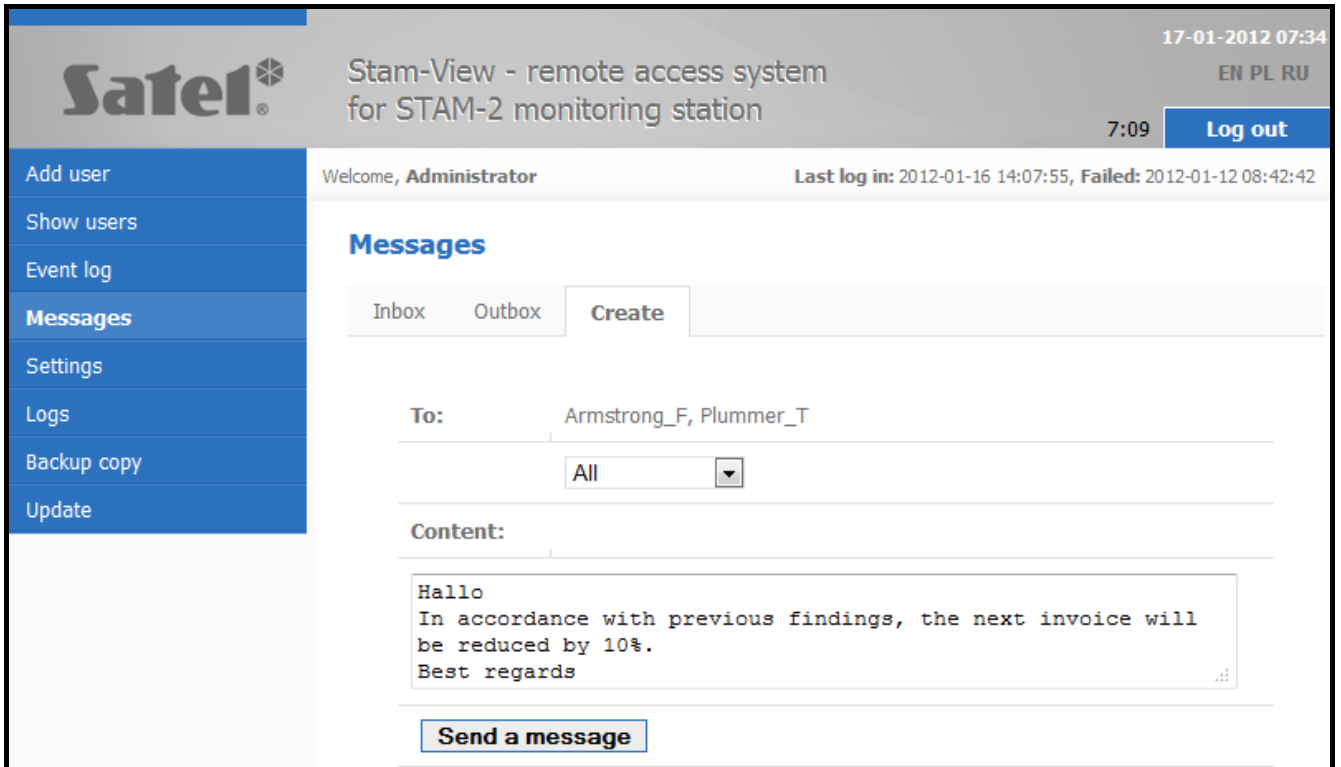
⌵ Change filter parameters

Date	Type	Information	Video
2012-02-06 15:00:50	Log out	Connection has been terminated...	
2012-02-06 14:58:03	Log in	User logged into the system: s...	
2012-02-06 14:56:48	Information	Logging attempt by: satel	
2012-02-06 14:03:11	Arming	Arm	
2012-02-06 14:03:08	Information	End of need for medical suppor...	
2012-02-06 14:03:07	Alarm	Medical support needed	
2012-02-06 14:02:58	Disarming	Disarm	
2012-02-06 14:02:57	Alarm	Burglary	
2012-02-06 14:02:04	Log in	User logged into the system: r...	
2012-02-06 14:01:50	Information	Start server	

<< previous page 2 from 217 next >>  
 Results per page 10

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.

The screenshot displays the SATEL Stam-View web interface. The top header includes the SATEL logo, the text "Stam-View - remote access system for STAM-2 monitoring station", the date and time "17-01-2012 07:37", and language options "EN PL RU". A "Log out" button is visible in the top right. The left sidebar contains navigation links: "Add user", "Show users", "Event log", "Messages", "Settings" (highlighted), "Logs", "Backup copy", and "Update". The main content area shows a "Welcome, Administrator" message and a "Last log in" status. The "Settings" section is active, with tabs for "Password", "Logo", "Users" (selected), "Installers", "SSL Certificates", and "Languages". Under "Users", there are two sections: "Deleting messages" with a checked checkbox, and "Events types" with a list of checkboxes for various event types. A "Save" button is located at the bottom of the settings area.

17-01-2012 07:37  
EN PL RU  
9:53 **Log out**

Add user  
Show users  
Event log  
Messages  
**Settings**  
Logs  
Backup copy  
Update

Welcome, **Administrator** **Last log in:** 2012-01-16 14:07:55, **Failed:** 2012-01-12 08:42:42

### Settings

Password Logo **Users** Installers SSL Certificates Languages

Deleting messages

Events types

<input checked="" type="checkbox"/> Alarm	<input checked="" type="checkbox"/> Arming
<input checked="" type="checkbox"/> Disarming	<input checked="" type="checkbox"/> Trouble
<input checked="" type="checkbox"/> Test	<input type="checkbox"/> Remark
<input checked="" type="checkbox"/> Information	<input type="checkbox"/> Comment
<input checked="" type="checkbox"/> False alarm	<input checked="" type="checkbox"/> Invalid disarming
<input type="checkbox"/> Log in	<input type="checkbox"/> Log out
<input type="checkbox"/> SMS	<input type="checkbox"/> Telephone

**Save**

- 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.

17-01-2012 07:39  
EN PL RU  
9:20 **Log out**

**Satel** Stam-View - remote access system for STAM-2 monitoring station

Welcome, **Administrator** Last log in: 2012-01-16 14:07:55, Failed: 2012-01-12 08:42:42

**Backup copies**

Copies Upload

**Available backup copies**

Date of creating	Actions
2011-08-19 11:39:29	🗑️ ⬇️ ⬆️
2011-11-28 07:39:43	🗑️ ⬇️ ⬆️
2012-01-07 08:34:35	🗑️ ⬇️ ⬆️

[Make a new one](#)

- Viewing the STAM-VIEW related system events.

17-01-2012 14:22  
EN PL RU  
9:29 **Log out**

**Satel** Stam-View - remote access system for STAM-2 monitoring station

Welcome, **Administrator** Last log in: 2012-01-17 14:20:09, Failed: Never

**System logs**

Date	Action	Description
2012-01-17 14:22:06	User logged in	Administrator
2012-01-17 14:21:48	User logged in	Derek_O
2012-01-17 14:21:21	User logged in	Cimino_D
2012-01-17 14:20:54	User logged in	Cameron_C
2012-01-17 14:19:39	User logged in	Armstrong_F
2012-01-17 14:19:22	Failed login attempt	Armstrong_F
2012-01-17 14:19:03	User logged in	Brown_P
2012-01-17 14:18:47	User added	Armstrong_F
2012-01-17 14:18:11	Password changed	Caine_R
2012-01-17 14:17:22	Site assigned	Site: 8 to: Brown_P

page 1 from 10 next >>  
Results per page 10

10. Updating the STAM-VIEW system.

The screenshot displays the web interface for the Stam-View system. At the top left is the Satel logo. The main header area contains the text "Stam-View - remote access system for STAM-2 monitoring station" and a "Log out" button. The top right corner shows the date and time "17-01-2012 07:45" and language options "EN PL RU". A navigation menu on the left lists various system functions, with "Update" highlighted. The main content area shows a welcome message for the Administrator, the current version number "28102011", and a link to update the system.

<b>Satel</b>	Stam-View - remote access system for STAM-2 monitoring station	17-01-2012 07:45 EN PL RU
9:25	<b>Log out</b>	
Add user	Welcome, <b>Administrator</b>	<b>Last log in:</b> 2012-01-16 14:07:55, <b>Failed:</b> 2012-01-12 08:42:42
Show users	<b>Update</b>	
Event log	Current version:	<b>28102011</b>
Messages	<a href="#">Click here tu update</a>	
Settings		
Logs		
Backup copy		
<b>Update</b>		