



**System zdalnego dostępu
do stacji monitorującej STAM-2**

STAM-VIEW

Instrukcja instalacji systemu

stam-view_i_pl 10/11

SATEL sp. z o.o.
ul. Schuberta 79
80-172 Gdańsk
POLSKA
tel. 58 320 94 00
serwis 58 320 94 30
dz. techn. 58 320 94 20; 604 166 075
info@satel.pl
www.satel.pl

Firma SATEL stawia sobie za cel nieustanne podnoszenie jakości swoich produktów, co może skutkować zmianami w ich specyfikacji technicznej i oprogramowaniu. Aktualna informacja o wprowadzanych zmianach znajduje się na naszej stronie internetowej.

Proszę nas odwiedzić:

<http://www.satel.pl>

Zadaniem systemu STAM-VIEW jest rozbudowa funkcjonalności stacji monitorującej STAM-2. Wzbogaca ofertę kierowaną do abonentów stacji, umożliwiając uzyskanie dostępu do zdarzeń oraz sekwencji video spływających z monitorowanych obiektów przy pomocy przeglądarki www. Rozwiązanie to jest dodatkowym udogodnieniem dla klientów firm zajmujących się monitoringiem i ochroną. Równocześnie ułatwia ono pracę operatorom stacji monitorującej, którzy nie muszą się już angażować w przekazywanie informacji dotyczących stanu obiektów. Dystrybuowany jest w postaci wirtualnej maszyny opartej na technologii firmy VMware.

1. Właściwości

- Dostęp przy pomocy przeglądarki www.
- Możliwość zdalnego przeglądu zdarzeń.
- Możliwość weryfikacji stanu obiektu na odległość.
- Możliwość przeglądu sekwencji obrazów przesyłanych przez moduł Viver.
- Łatwy sposób testowania komunikacji systemu alarmowego podczas jego uruchamiania oraz okresowej konserwacji.
- Możliwość filtrowania zdarzeń.
- Szyfrowana transmisja.
- Definiowanie przez administratora uprawnień dla użytkowników oraz instalatorów.
- Komunikacja wewnętrzna pomiędzy użytkownikami oparta o system wiadomości.
- Możliwość wykonania kopii zapasowej ustawień systemu.
- Niezależna baza danych.

2. Instalacja systemu

STAM-VIEW pracuje na platformie systemu VMware ESXi, do którego zarządzania i administrowania służy program VMware vSphere Client. Oba programy należy pobrać ze strony producenta <http://downloads.vmware.com/>.

Oprogramowanie firmy VMware to aplikacja umożliwiająca wirtualizację wielu systemów operacyjnych na jednej fizycznej maszynie. Systemy uruchamiane jako wirtualne mogą komunikować się między sobą za pośrednictwem protokołów internetowych. Takie rozwiązanie umożliwia zaoszczędzenie miejsca, ograniczenie kosztów zakupu nowego sprzętu, redukcję kosztów zasilania oraz chłodzenia. Zwiększa również dostępność aplikacji oraz zapewnia wysoki poziom ochrony danych.

2.1 Wymagania dotyczące sieci

- Sieć lokalna w klasie adresowej 192.168.1.0/24 (adresy od 192.168.1.1 – 192.168.1.254, net maska 255.255.255.0).
- Stacja monitorująca, z którą komunikuje się STAM-VIEW, powinna mieć adres IP w tej samej podsieci.
- 2 wolne adresy IP: jeden dla wirtualnej maszyny STAM-VIEW - 192.168.1.123, drugi (dowolny) dla systemu VMware ESXi.
- Router o adresie IP z sieci lokalnej – 192.168.1.1, odpowiednio skonfigurowany do przekierowania portu https (443) na adres 192.168.1.123, żeby serwis był dostępny z internetu (instalacja routera jest konieczna w przypadku braku wolnego adresu IP 192.168.1.123).

2.2 Minimalne wymagania sprzętowe dla serwera, na którym zostanie zainstalowany system VMware ESXi

- Procesor 64-bitowy z rodziny:
Intel Xeon seria: 3000/3200, 3100/3300, 5100/5300, 5200/5400, 7100/7300, 7200/7400,
Intel Nehalem,
AMD Opteron.
- 2 GB pamięci RAM (**zalecane 4 GB pamięci RAM**).
- Karta sieciowa 1GB lub 10GB (**zalecana karta Intel Pro 1000**).
- Jeden lub więcej kontrolerów SCSI (**np. kontroler Adaptec 2405**).
- Macierz dyskowa (skonfigurowana w trybie RAID 1).

Uwaga: Sprzęt, na którym zainstalowany zostanie system VMware ESXi, musi się znajdować na liście dostępnej na stronie <http://www.vmware.com/resources/compatibility/search.php>.

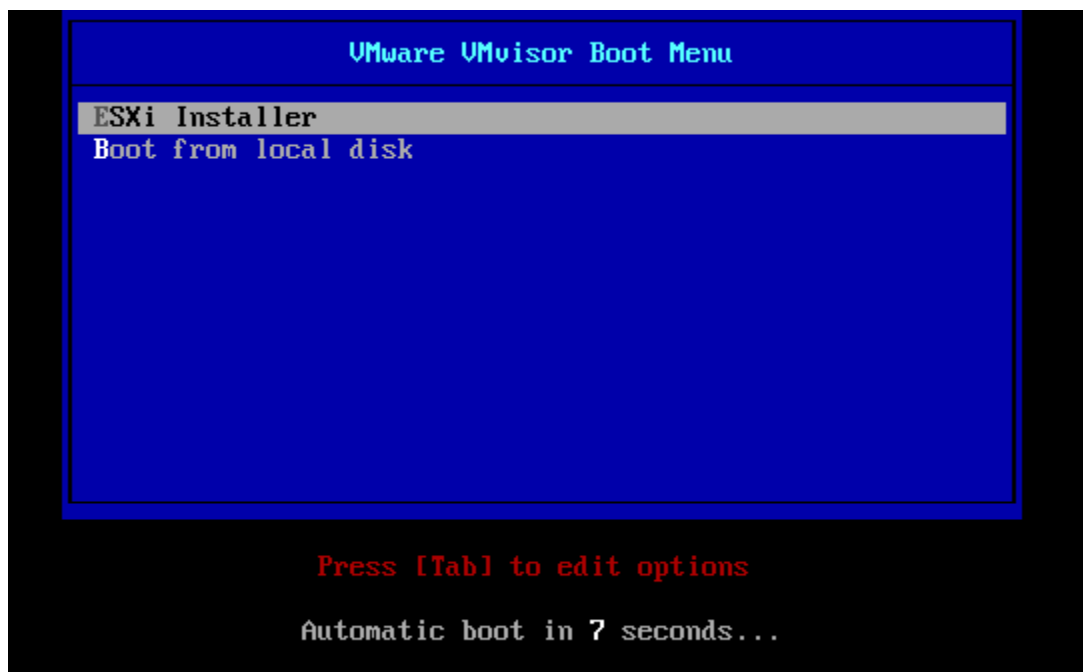
2.3 Pobieranie plików

Na stronie producenta <http://downloads.vmware.com/> należy wybrać pozycję VMware vSphere Hypervisor (ESXi), a następnie kliknąć przycisk „Download”. Wyświetli się strona do rejestracji w bazie danych. Rejestracja jest konieczna do darmowego pobierania plików oraz do uzyskania darmowej licencji dla systemu VMware ESXi oraz dla programu VMware vSphere Client. Dalej należy postępować zgodnie z zaleceniami producenta.

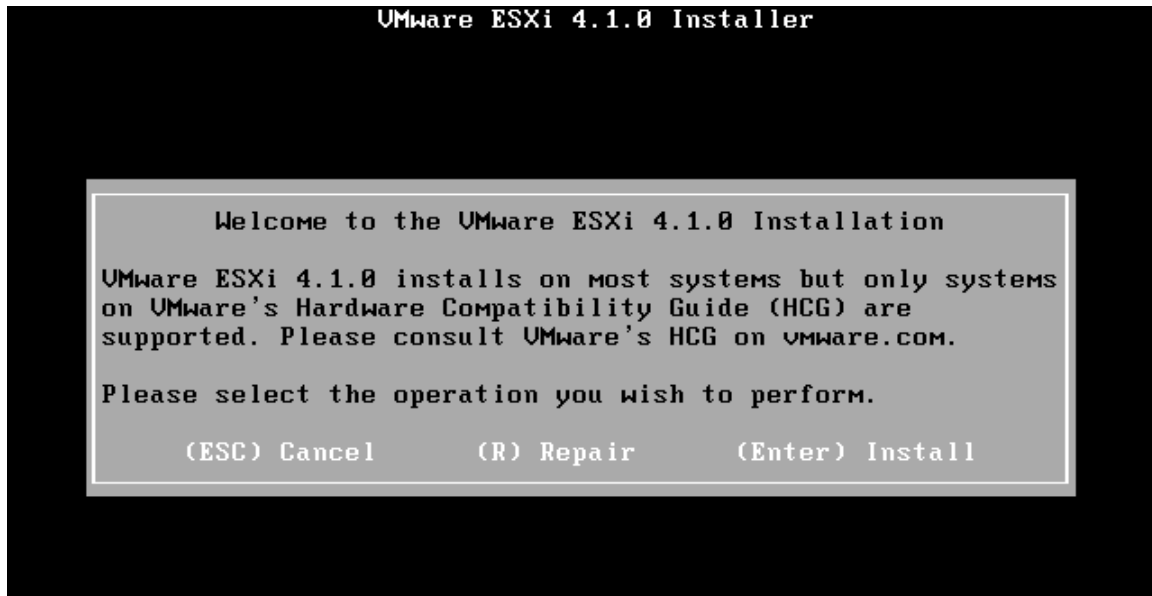
Po pobraniu obrazu ISO należy nagrać go na płytę CD. Nagrana płyta umożliwi instalację systemu VMware ESXi na przeznaczonym do tego serwerze.

2.4 Instalacja systemu operacyjnego VMware ESXi

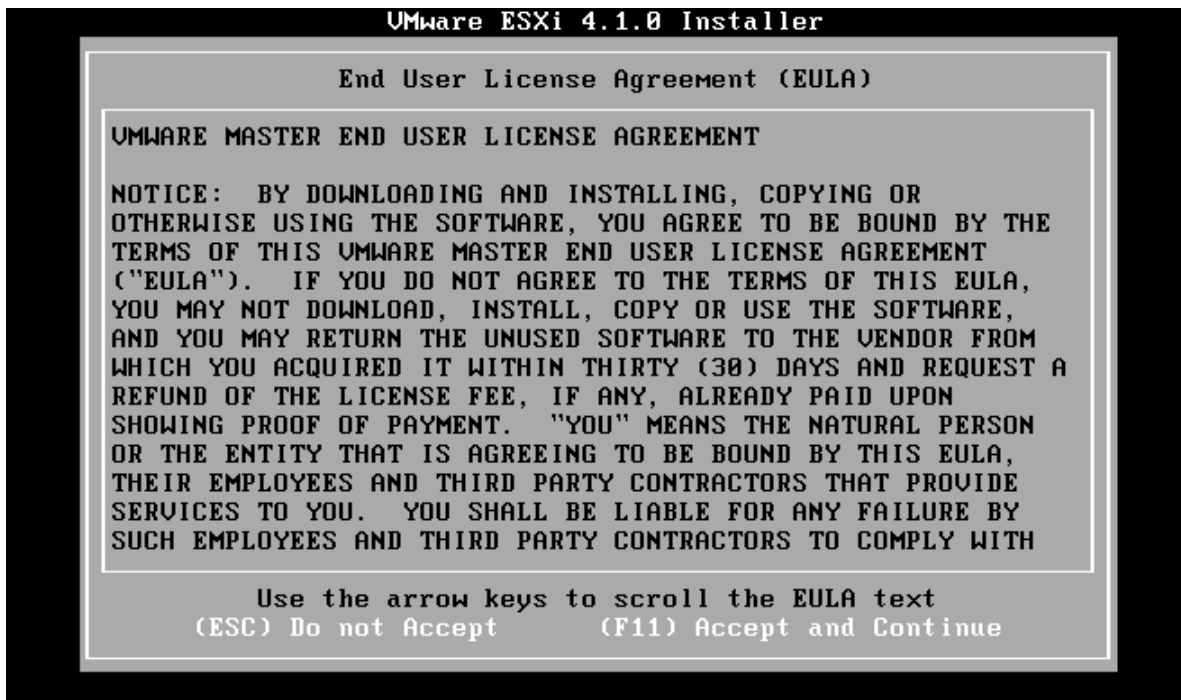
1. Włączyć serwer i włożyć do napędu nagraną płytę CD.
2. Wybrać opcję ESXi Installer i zatwierdzić naciskając ENTER.



3. Pojawi się komunikat informujący, że system można instalować tylko na sprzęcie spełniającym wymagania opisane wcześniej w niniejszej instrukcji. Nacisnąć ENTER w celu kontynuowania instalacji.



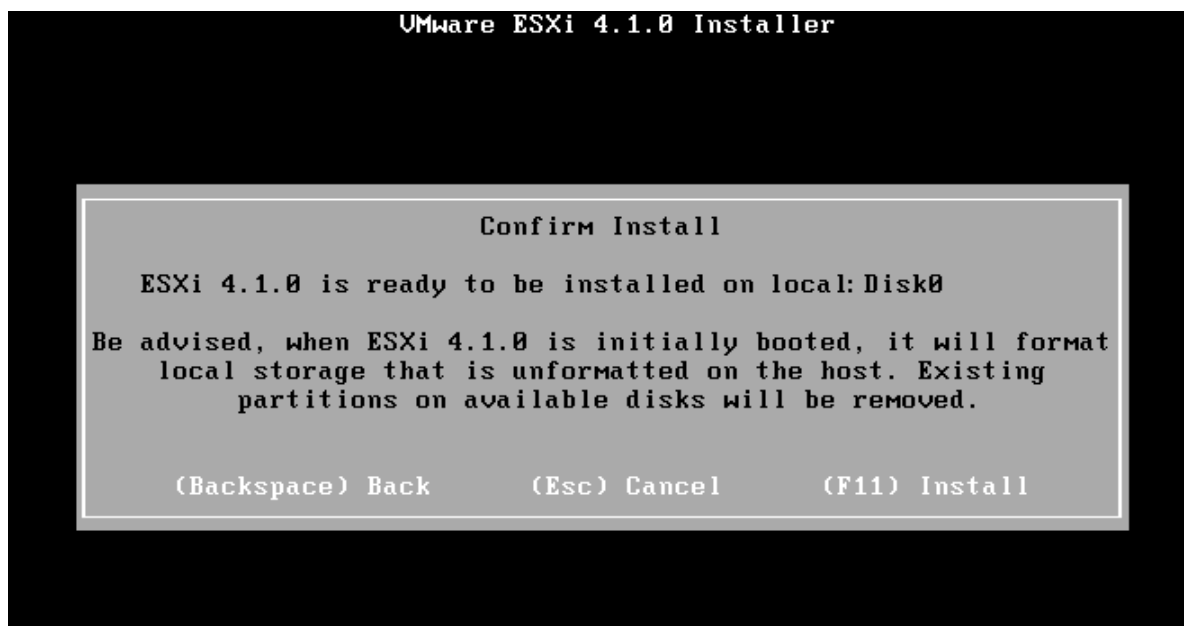
4. Po przeczytaniu warunków licencji, zaakceptować je naciskając F11.



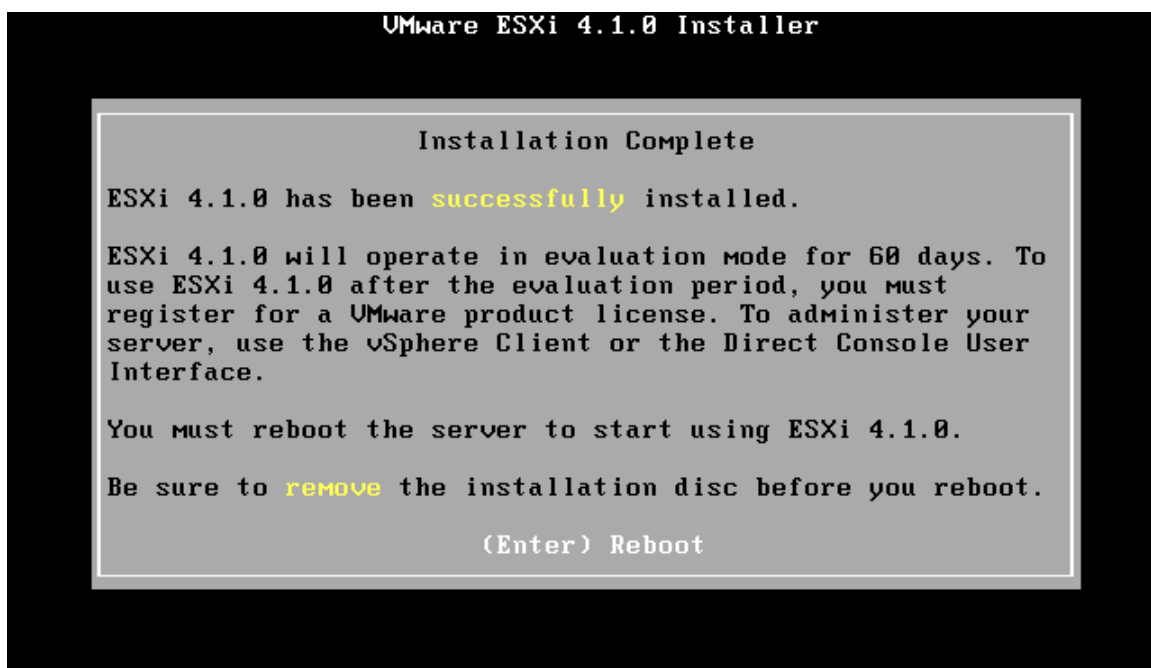
5. Wyświetli się lista dostępnych na serwerze dysków. Wybrać ten, na którym ma zostać zainstalowany system operacyjny i zatwierdzić naciskając ENTER.



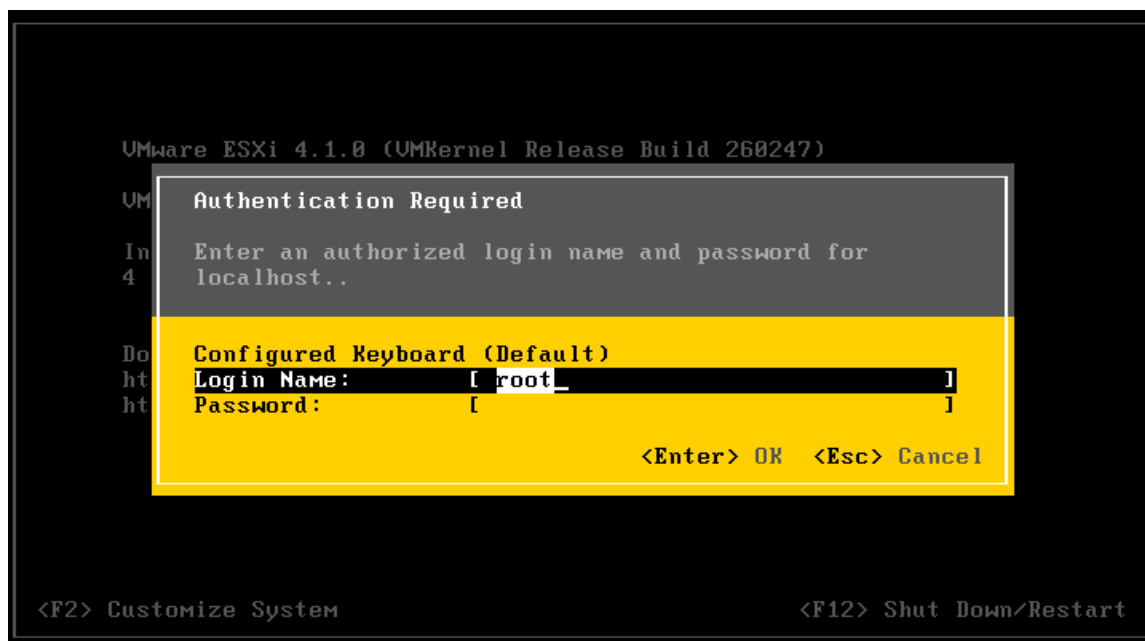
6. Nacisnąć F11, aby uruchomić kolejne etapy instalacji.



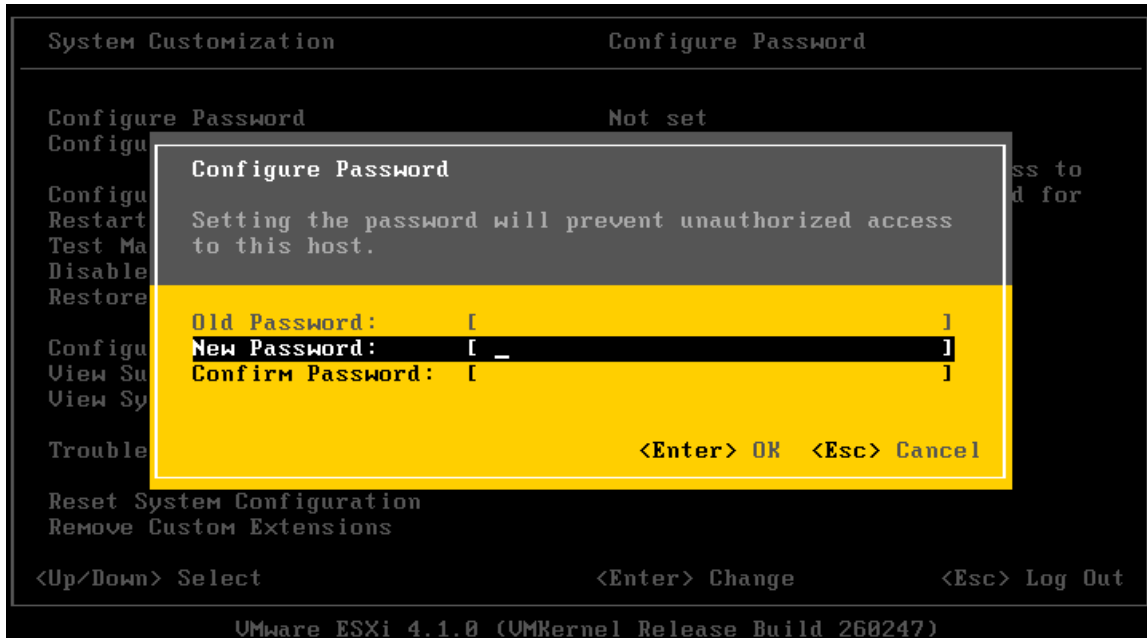
- Po zakończonej instalacji należy wyjąć płytę CD z napędu, a następnie nacisnąć ENTER w celu zrestartowania komputera.



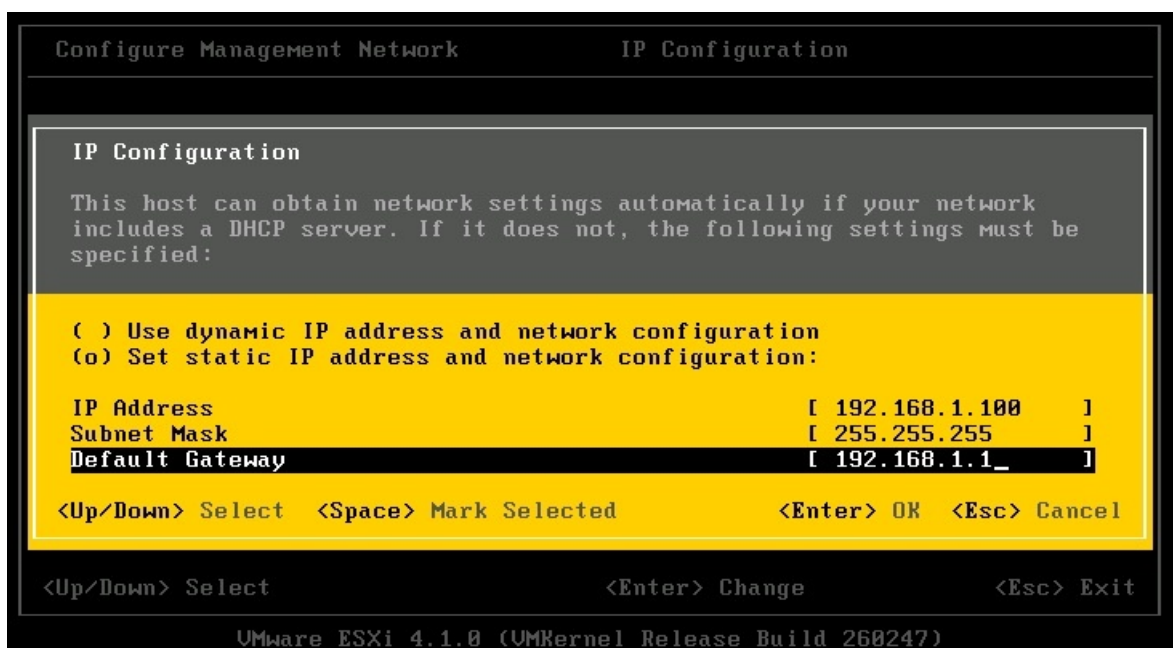
- Po zainstalowaniu systemu operacyjnego VMware ESXi i zrestartowaniu komputera wyświetli się okno „Authentication Required”. Należy nacisnąć ENTER akceptując wpisane już dane i przejść do kolejnego okna.



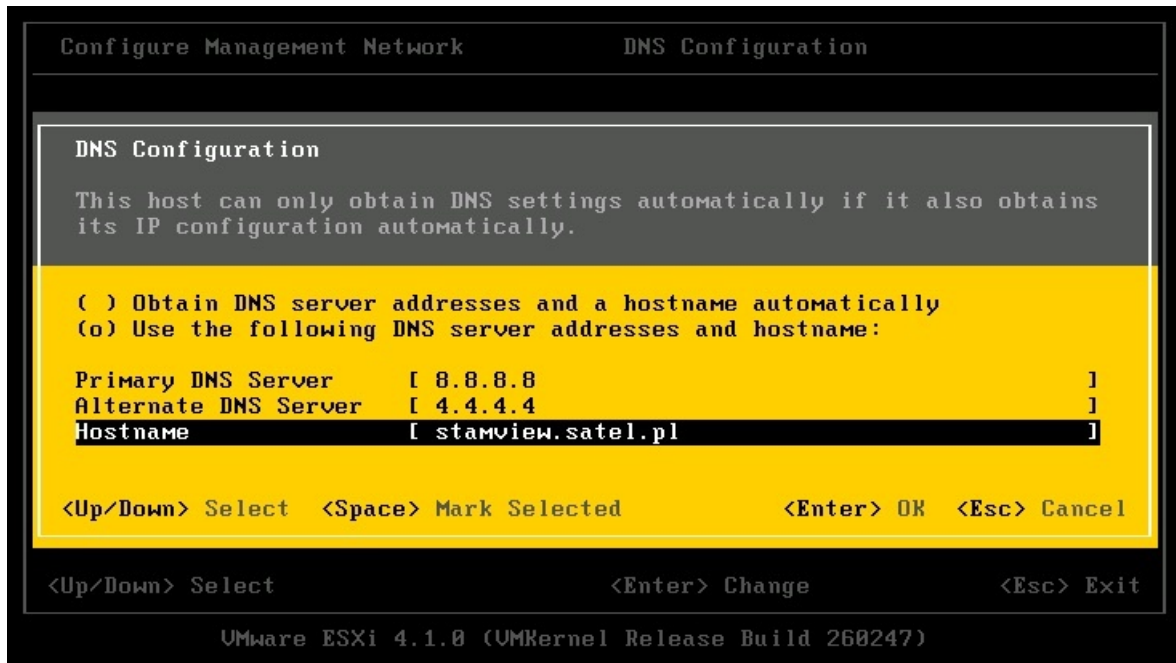
9. Nacisnąć F2, żeby przejść do podstawowej konfiguracji serwera oraz do jego ustawień sieciowych. Wybrać polecenie „Configure Password” i zdefiniować hasło do serwera. Hasło może liczyć od 8 do 40 znaków (litera i cyfry). Zatwierdzić wprowadzone zmiany naciskając ENTER. Powrót do głównego menu ustawień serwera nastąpi po naciśnięciu ESC.



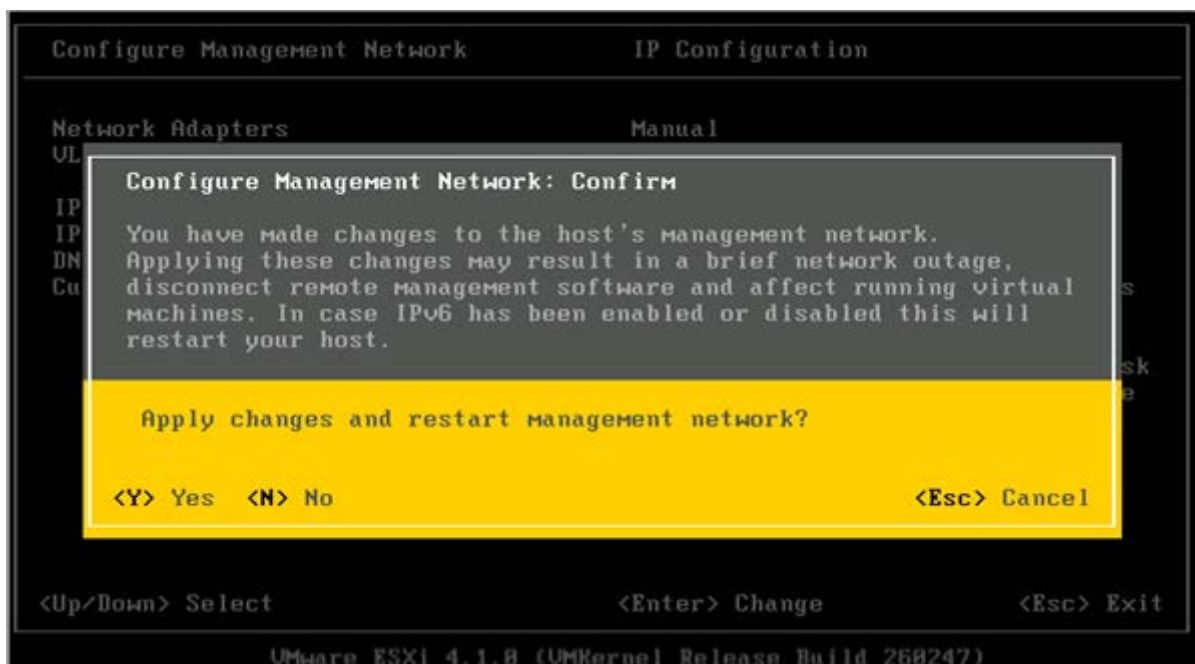
10. Wybrać polecenie „Configure Management Network”, a w nim „IP Configuration”. Jeżeli adres sieciowy jest przydzielany serwerowi dynamicznie przez serwer DHCP, zostawić zaznaczoną opcję „Use dynamic IP address and network configuration”. Jeżeli adres sieciowy serwera ma być wprowadzony ręcznie, zaznaczyć opcję „Set static IP address and network configuration” i wpisać odpowiednie dane w polach „IP Address”, „Subnet Mask” oraz „Default Gateway”. Zatwierdzić wprowadzone zmiany naciskając ENTER. Następnie nacisnąć ESC, żeby wrócić do głównego menu ustawień serwera. Podane poniżej dane są przykładowe.



11. Jeżeli ustawienia sieciowe zostały wprowadzone ręcznie, należy skonfigurować również adres serwera DNS. Wybrać polecenie „DNS Configuration” i w polach „Primary DNS Server”, „Alternate DNS Server” wpisać adresy IP serwera DNS, a w polu „Hostname” – nazwę serwera VMware ESXi. Zatwierdzić wprowadzone zmiany naciskając ENTER. Powrót do głównego menu ustawień serwera nastąpi po naciśnięciu ESC. Podane poniżej dane są przykładowe.

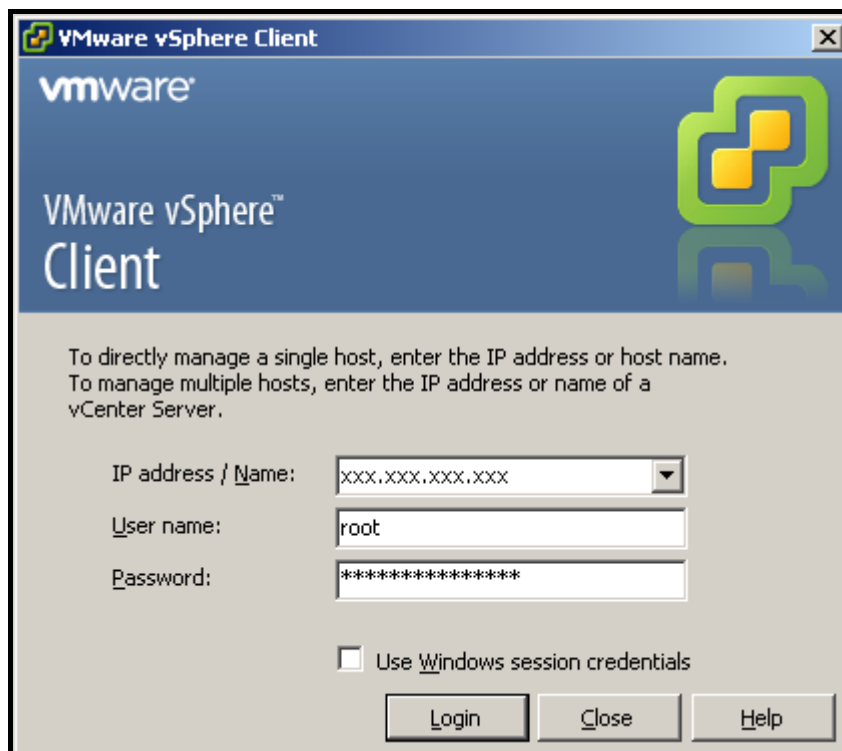


12. Po wprowadzeniu danych sieciowych nacisnąć ESC, żeby wyjść z menu, a następnie zatwierdzić nowe ustawienia naciskając „Y”.

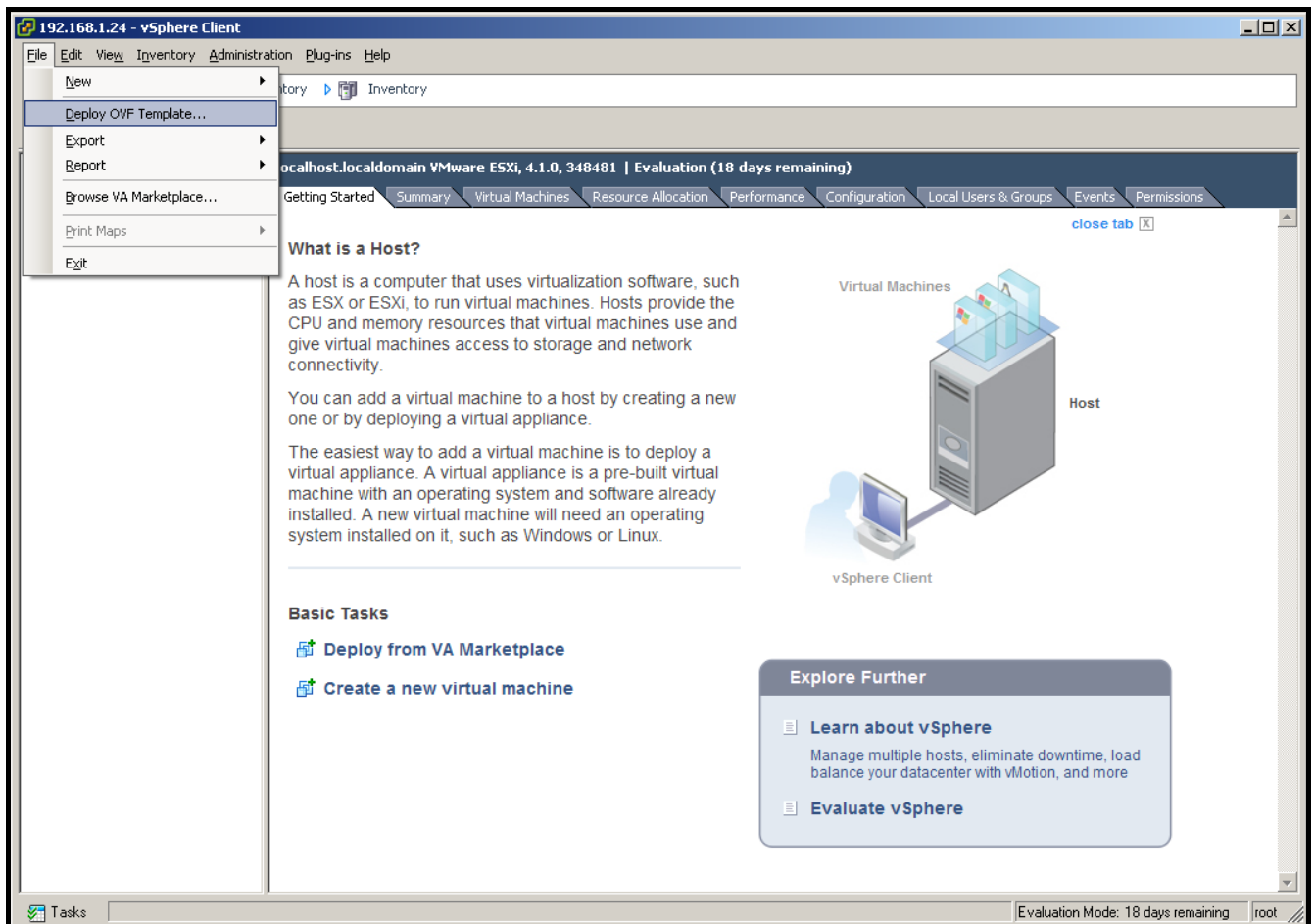


2.5 Instalacja oprogramowania VMware vSphere Client

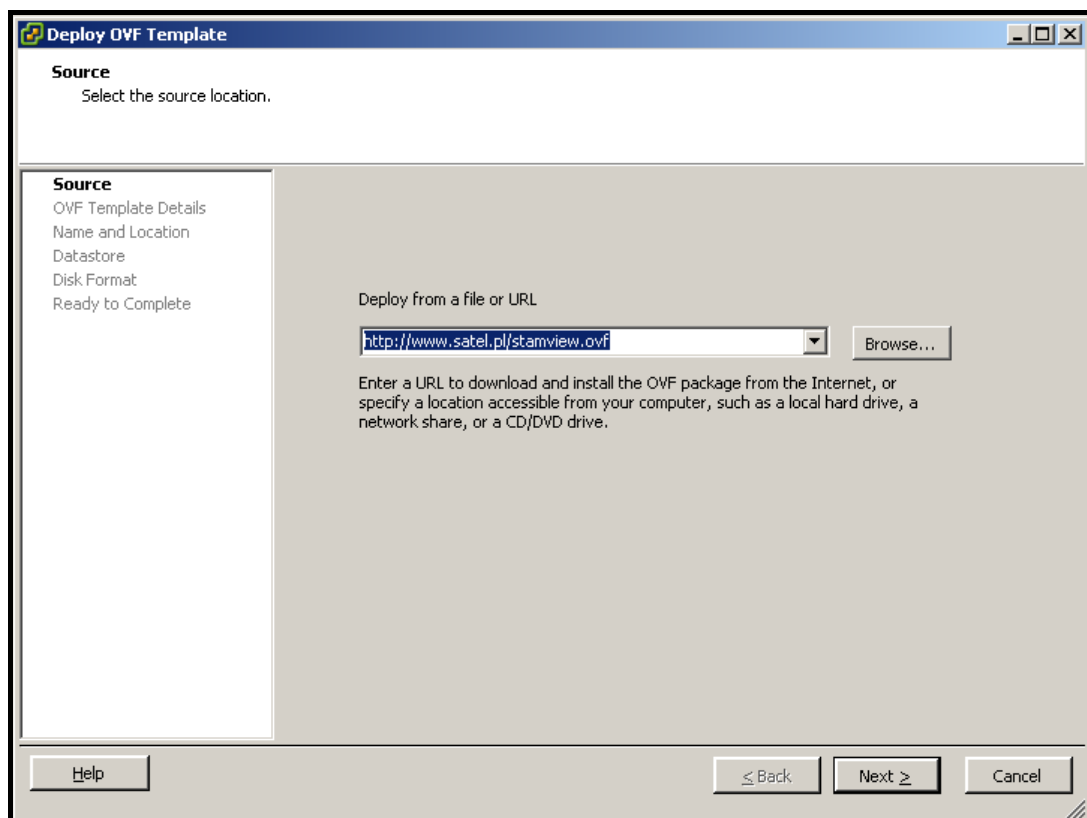
1. Otworzyć okno przeglądarki internetowej i wpisać adres IP serwera VMware ESXi. Po połączeniu kliknąć na link „Download vSphere Client”. Uruchomi się instalacja oprogramowania.
2. Po zakończeniu instalacji, uruchomić program, klikając na skrót programu utworzony na pulpicie lub w Menu Start.
3. Podczas logowania podać:
IP address / Name: wpisać adres IP lub nazwę serwera, na którym zainstalowano system VMware ESXi,
User name: wpisać „root”,
Password: wpisać hasło wprowadzone podczas konfiguracji serwera VMware ESXi.



4. Wybrać z menu „File” polecenie „Deploy OVF Template”.



5. W polu „Deploy from a file or URL” wpisać adres: <http://www.satel.pl/stamview.ovf> i nacisnąć NEXT.



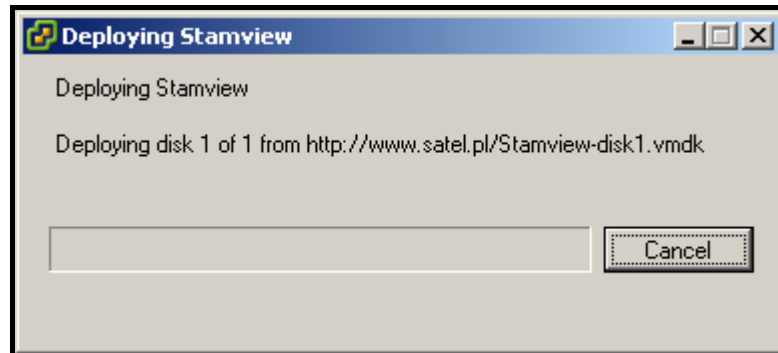
6. Wpisać nazwę maszyny wirtualnej ze STAM-VIEW i nacisnąć NEXT.

The screenshot shows the 'Deploy OVF Template' wizard window. The title bar says 'Deploy OVF Template'. The main heading is 'Name and Location' with the instruction 'Specify a name and location for the deployed template'. On the left, there is a sidebar with links: 'Source', 'OVF Template Details', 'Name and Location' (which is highlighted), 'Datastore', 'Disk Format', and 'Ready to Complete'. The main area has a 'Name:' label and a text input field containing 'Stamview'. Below the input field, it says 'The name can contain up to 80 characters and it must be unique within the inventory folder.' At the bottom, there are three buttons: 'Help', '< Back', 'Next >', and 'Cancel'.

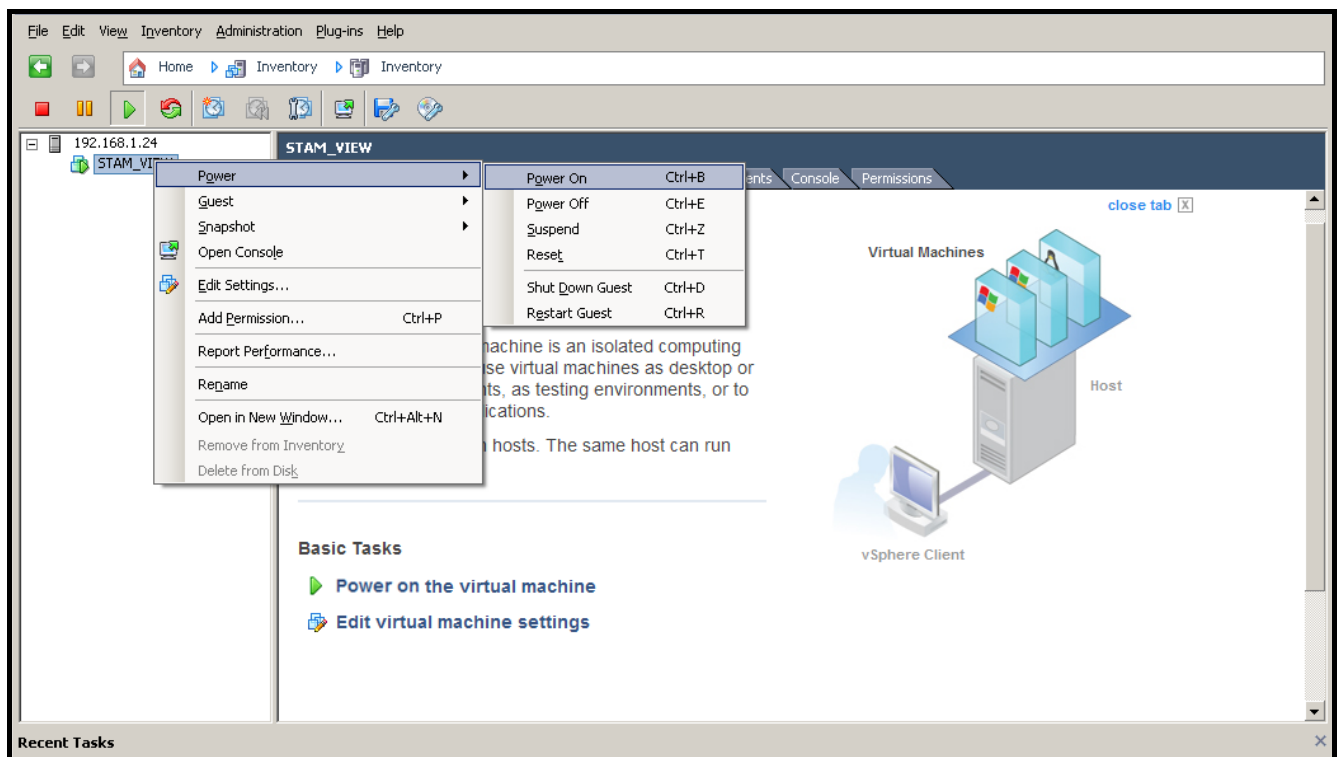
7. Wybrać dysk, na którym ma być umiejscowiona wirtualna maszyna i nacisnąć NEXT.
8. Zaznaczyć opcję „Thick provisioned format” i nacisnąć NEXT.

The screenshot shows the 'Deploy OVF Template' wizard window at the 'Disk Format' step. The title bar says 'Deploy OVF Template'. The main heading is 'Disk Format' with the instruction 'In which format do you want to store the virtual disks?'. On the left, the sidebar has links: 'Source', 'OVF Template Details', 'Name and Location', 'Datastore', 'Disk Format' (which is highlighted), and 'Ready to Complete'. The main area has a section 'Information about the selected datastore:' with the following details: Name: datastore2, Capacity: 927,3 GB, Free space: 926,7 GB. Below this, it says 'Select a format in which to store the virtual machines virtual disks:'. There are two radio button options: 'Thin provisioned format' (which is unselected) and 'Thick provisioned format' (which is selected). The 'Thin provisioned format' description says 'The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disks.' and 'Estimated disk usage: 1,9 GB'. The 'Thick provisioned format' description says 'All storage is allocated immediately.' and 'Estimated disk usage: 5,0 GB'. At the bottom, there are three buttons: 'Help', '< Back', 'Next >', and 'Cancel'.

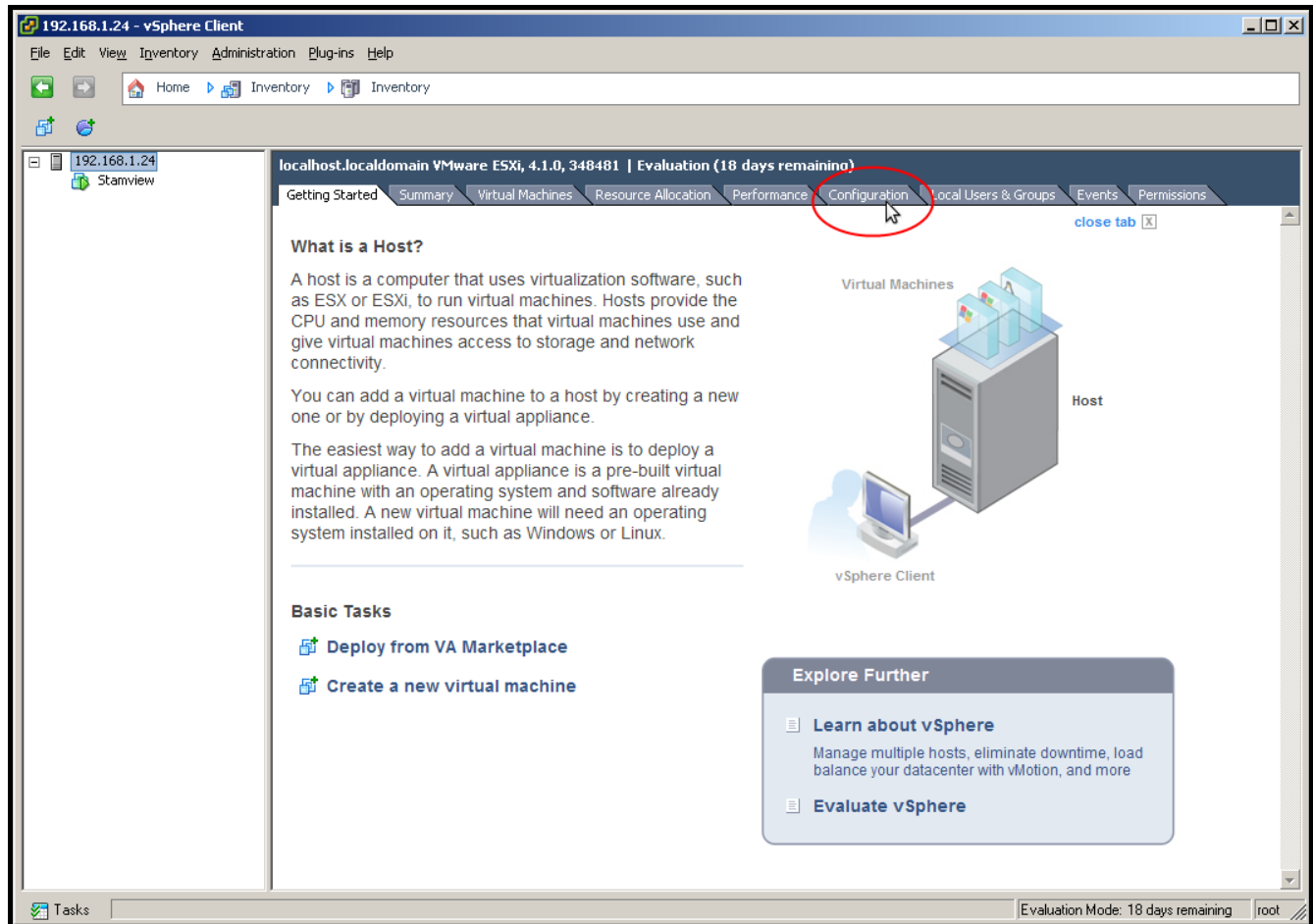
9. Wyświetli się podsumowanie danych dotyczących ustawień wirtualnej maszyny. Nacisnąć FINISH. Środowisko STAM-VIEW zajmuje ponad 530 MB, dlatego proces jego importowania może potrwać nawet ok. 1 godziny.



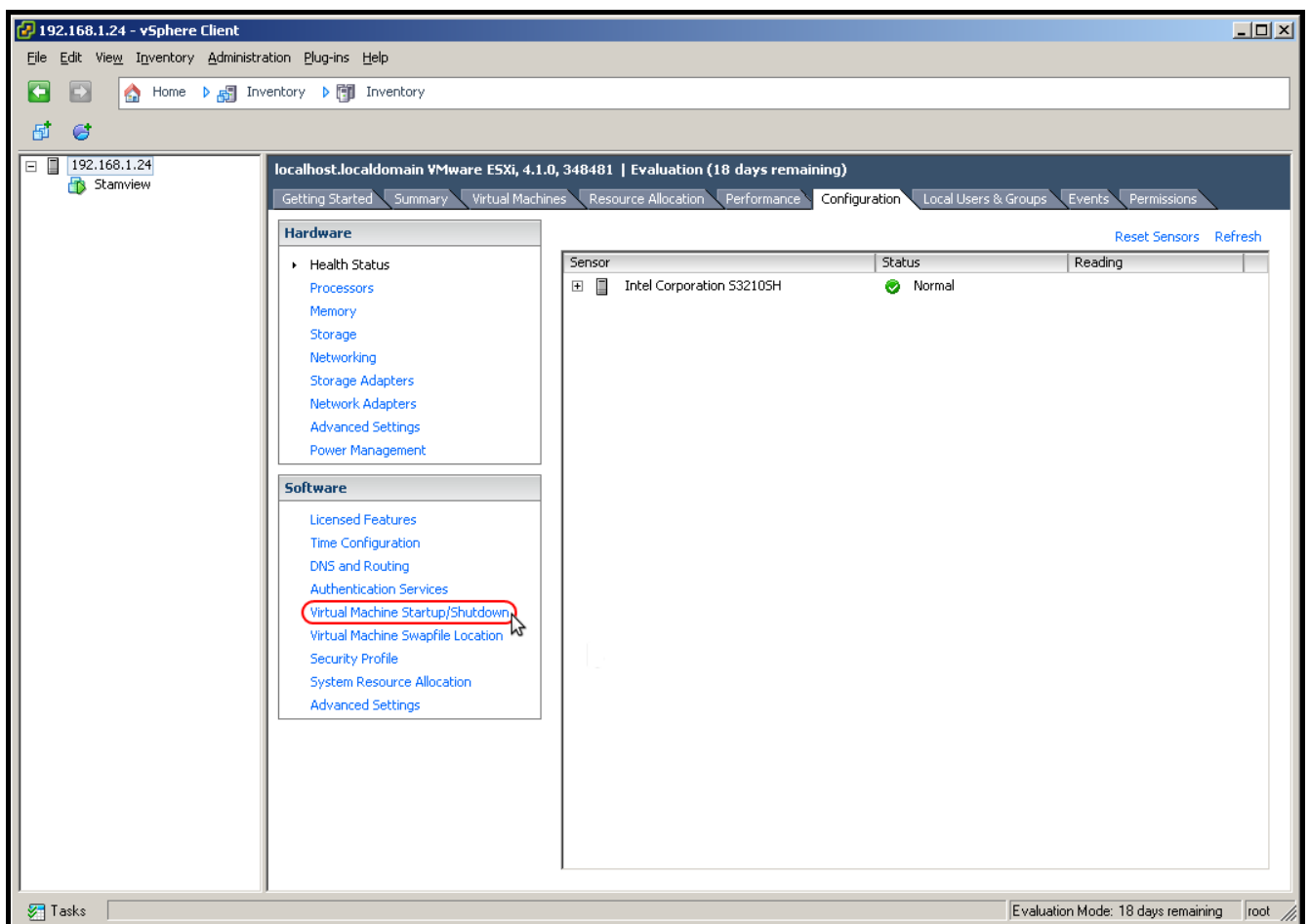
10. W celu uruchomienia zaimportowanej maszyny, ustawić kursor myszki na nazwie maszyny, kliknąć prawym przyciskiem myszki i w menu rozwijanym kliknąć polecenie „Power”, a następnie „Power On”. Widniejący na zrzucie adres IP maszyny, na której zainstalowano system STAM-VIEW, jest przykładowy.



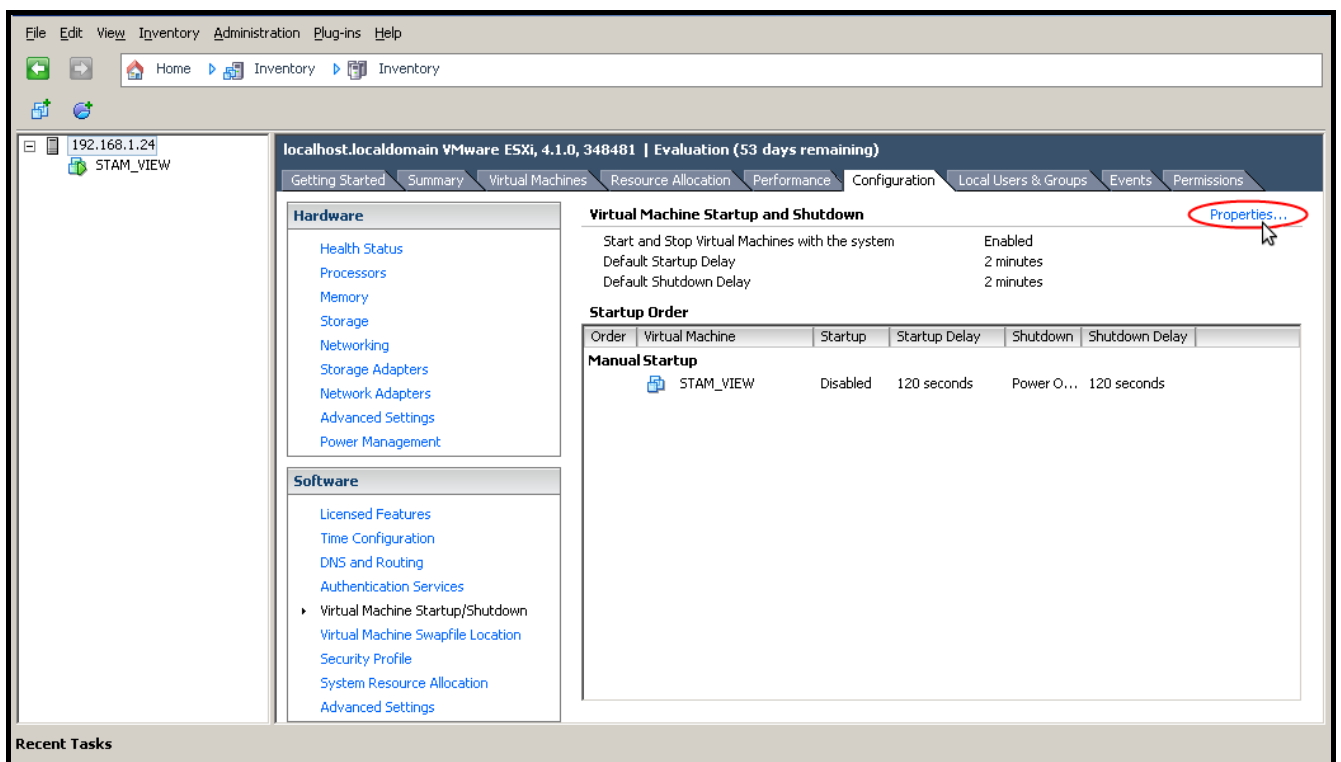
11. Włączyć automatyczne uruchamianie maszyny. W tym celu najechać kursorem myszki na adresie maszyny i kliknąć lewym przyciskiem myszki. Wyświetlą się zakładki z danymi dotyczącymi serwera. Wybrać zakładkę „Configuration”.



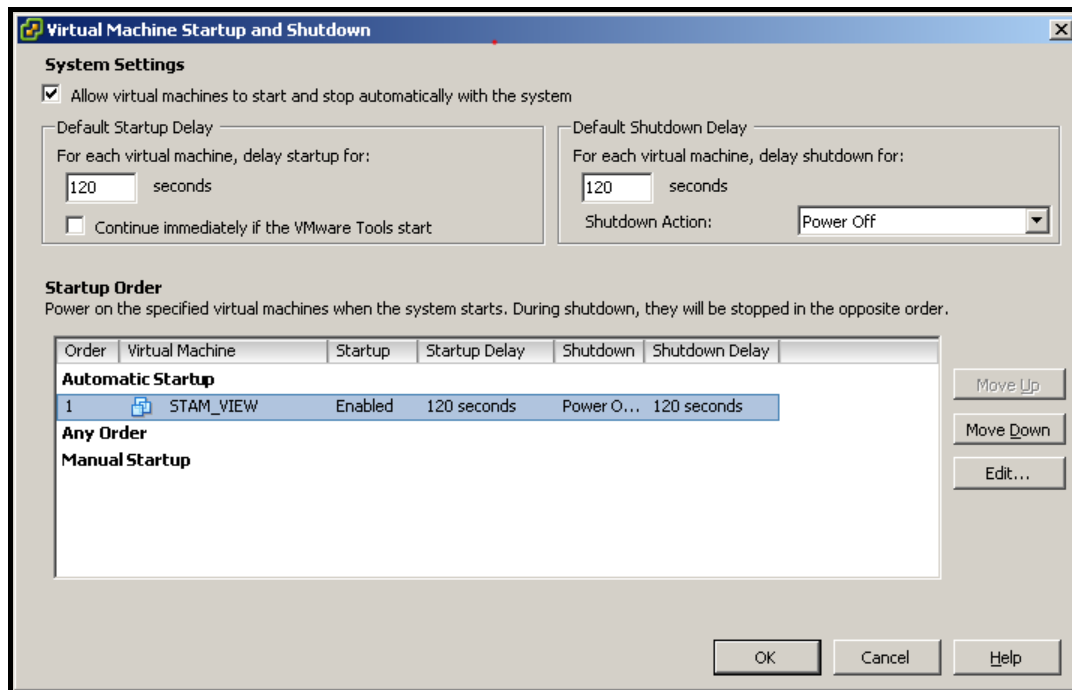
12. W części „Software” kliknąć na „Virtual Machine Startup/Shutdown”.



13. Wybrać funkcję „Properties” w prawym górnym rogu okna.



14. Zaznaczyć polecenie „Allow virtual machines to start and stop automatically with the system”. Następnie zaznaczyć wirtualną maszynę „STAMVIEW” i przy pomocy przycisku „Move Up” przenieść ją do obszaru o nazwie „Automatic Startup”.

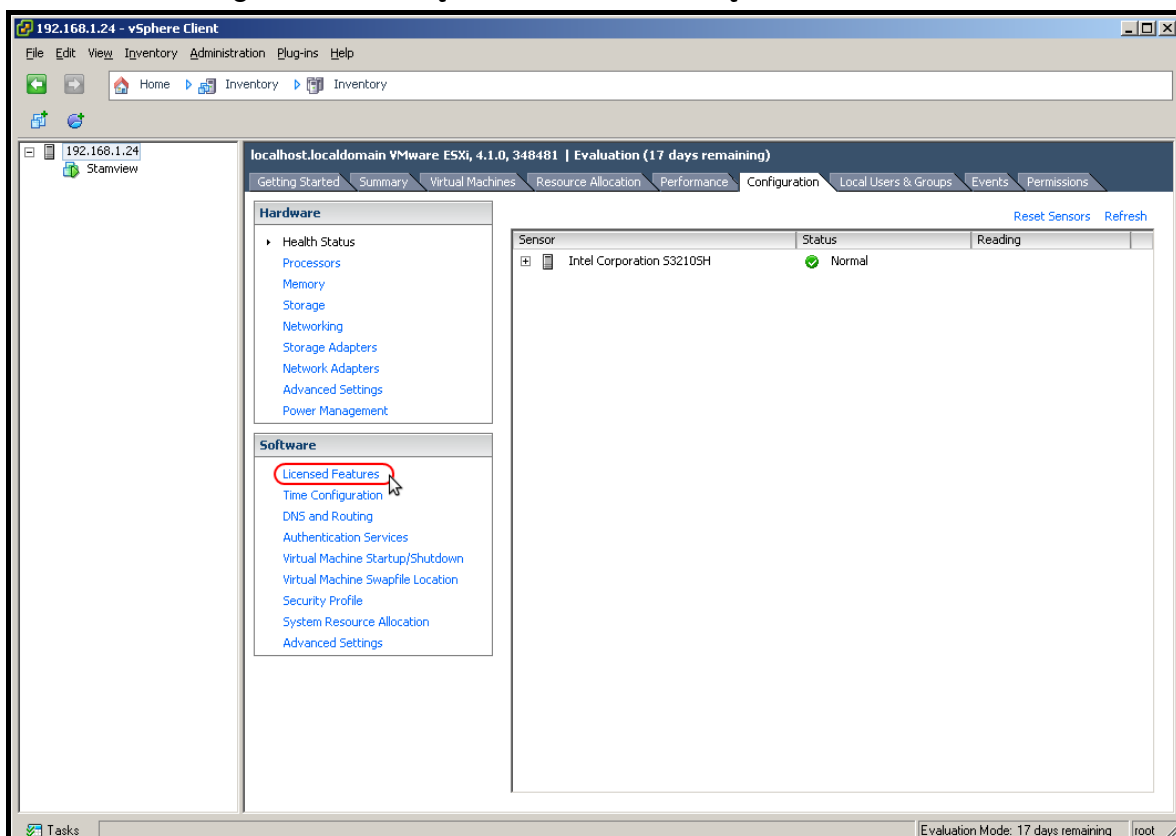


2.5.1 Wprowadzanie klucza licencyjnego

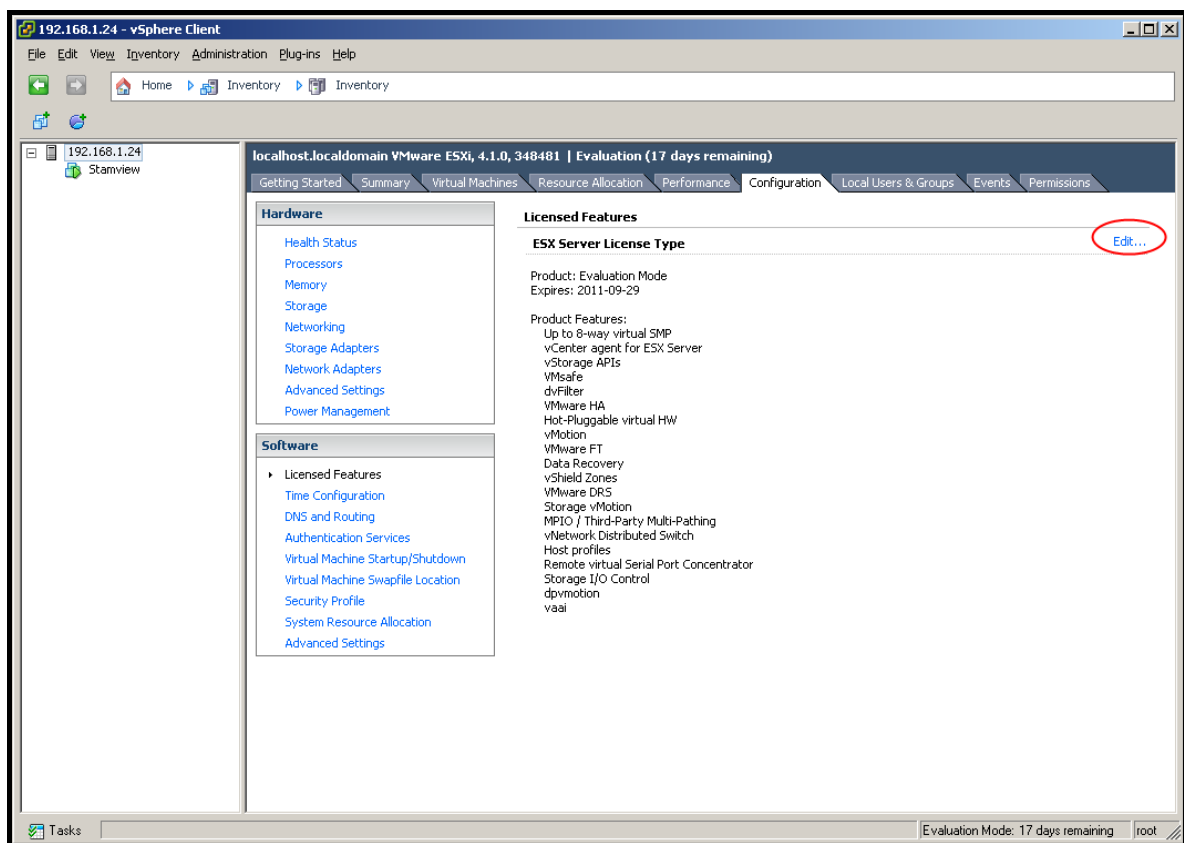


Należy pamiętać o wprowadzeniu klucza licencyjnego potrzebnego do prawidłowego działania programu powyżej 60 dni. Klucz jest dostępny po zalogowaniu się na swoje konto na stronie producenta oprogramowania VMware.

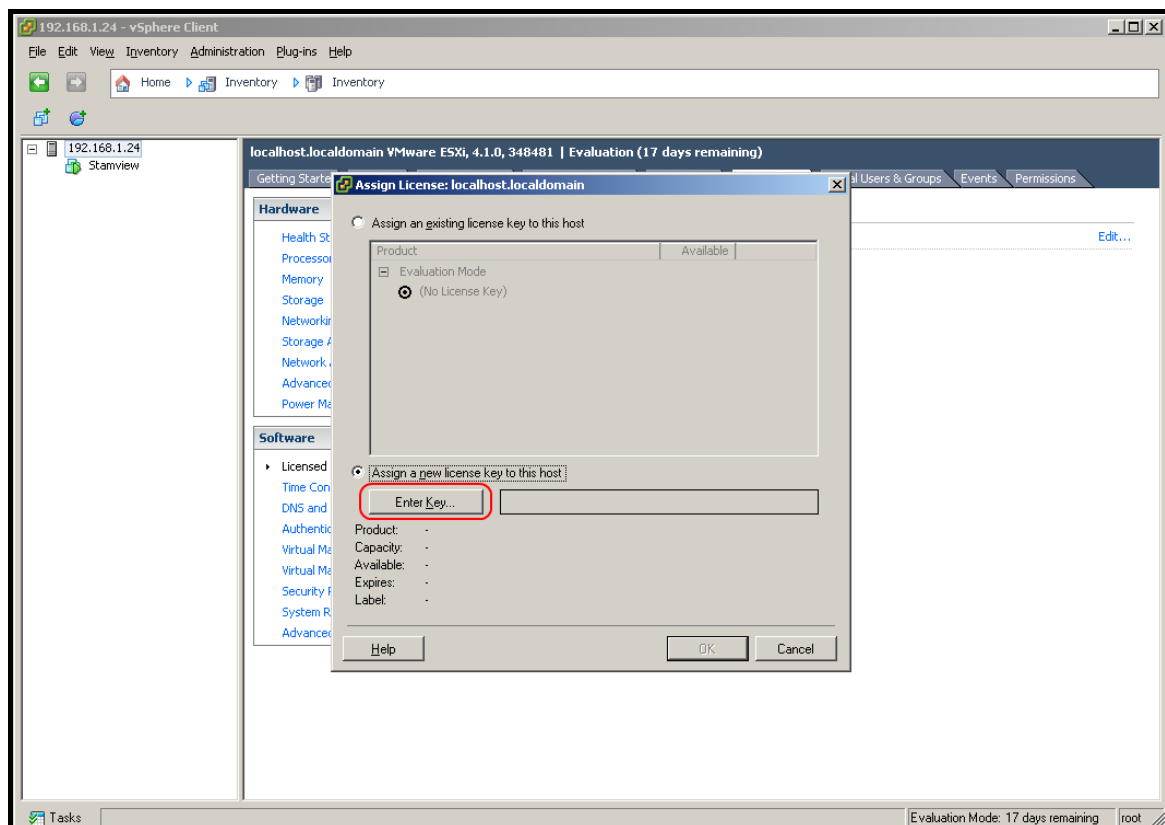
1. W zakładce „Configuration” w części „Software” kliknąć na „Licensed Features”.



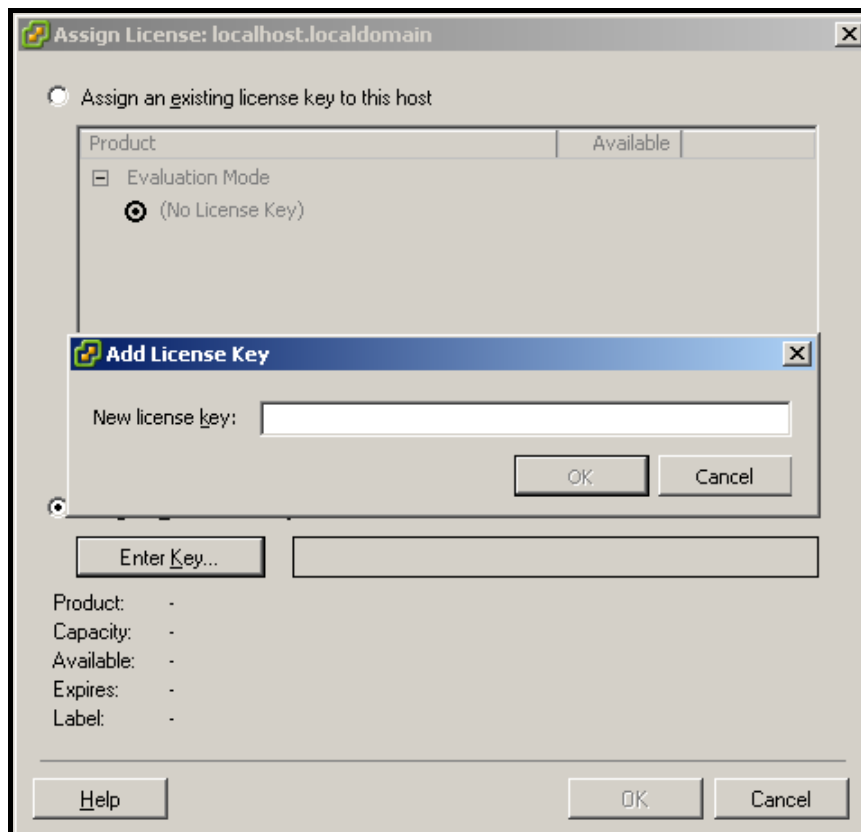
2. Wybrać funkcję „Edit...” w prawym górnym rogu okna.



3. Zaznaczyć polecenie „Assign a new license key to this host”. Kliknąć przycisk “Enter Key...”.



4. W oknie "Add License Key" w polu „New license key” wpisać kod. Kliknąć „OK”.



5. W oknie „Assign License” kliknąć „OK”.

3. Certyfikaty SSL

Wymagane jest wygenerowanie odpowiednich certyfikatów SSL potwierdzających bezpieczeństwo połączenia przeglądarki internetowej z serwerem. Po pierwszym zalogowaniu do systemu STAM-VIEW, przy ich statusie wyświetla się komunikat „Domyślny (wymagana zmiana)” dla certyfikatów SSL oraz „StartSSL” dla certyfikatów jednostki autoryzującej. Dlatego należy wygenerować odpowiedni certyfikat oraz klucz, a następnie wgrać je do systemu STAM-VIEW.

Uwagi:

- *Darmowy certyfikat SSL można uzyskać tylko będąc właścicielem domeny.*
- *Certyfikaty SSL będą działały prawidłowo tylko wtedy, gdy podczas instalacji adres serwera VMware ESXi zostanie podany w formie nazwy domeny.*

3.1 Certyfikaty firmy StartCom (zalecane)

W celu wygenerowania certyfikatu oraz klucza, administrator musi wykonać następujące czynności:

1. Wpisać w przeglądarce internetowej adres www.startssl.com.

2. W górnej lewej części okna wybrać zakładkę „StartSSL™ Products”.

The screenshot shows the StartSSL website interface. At the top, there are navigation links: StartCom Home, StartSSL PKI, StartSSL DNS, StartSSL WoT, F. A. Q., and Control Panel. The main heading is "StartSSL™ - The Swiss Army Knife of Digital Certificates & PKI". On the left sidebar, the "StartSSL™ Products" link is highlighted with a red arrow. Below it, there are sections for "StartSSL™ EV" (High Level Trust Indicator, Time Limited Offer, Only US\$199.90) and "SUPPORTED BROWSERS" (listing various browsers like Firefox, Chrome, etc.). The main content area is titled "Welcome to StartSSL™ PKI" and describes the services offered, including "StartSSL™ Free (Class 1)", "StartSSL™ Verified (Class 2)", "StartSSL™ Extended Validation", "Hardware", "Internationally Recognized", "High Protection", "Authentication", and "Easy Enrollment".

3. W części zatytułowanej „StartSSL™ Free” kliknąć na zielony panel z ikoną kłódki lub na odsyłacz „sign up”.

The screenshot shows the StartSSL website interface, specifically the "StartSSL™ Free" section. The left sidebar is visible, showing the "StartSSL™ Products" menu. The main content area is titled "StartSSL™ Free" and describes the services offered. A red arrow points to a green button labeled "...No Kidding 100% FREE". Below this button, there is a link to "sign up now for your StartSSL™ account and start to enjoy free digital certification immediately!". To the right, there is a section for "StartSSL™ Verified" which describes the services offered for a fee. At the bottom, there are sections for "StartSSL™ Extended Validation" and "StartSSL™ Web-of-Trust".

4. W oknie, które się otworzy, wybrać polecenie „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!

Authenticate

Sign-up

...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.

Express Lane

- 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. Przeczytać uważnie instrukcję zamieszczoną na stronie, wypełnić wszystkie pola niezbędne do rejestracji i kliknąć przycisk „Continue”.

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 *: ⓘ

Clear **Continue >>**

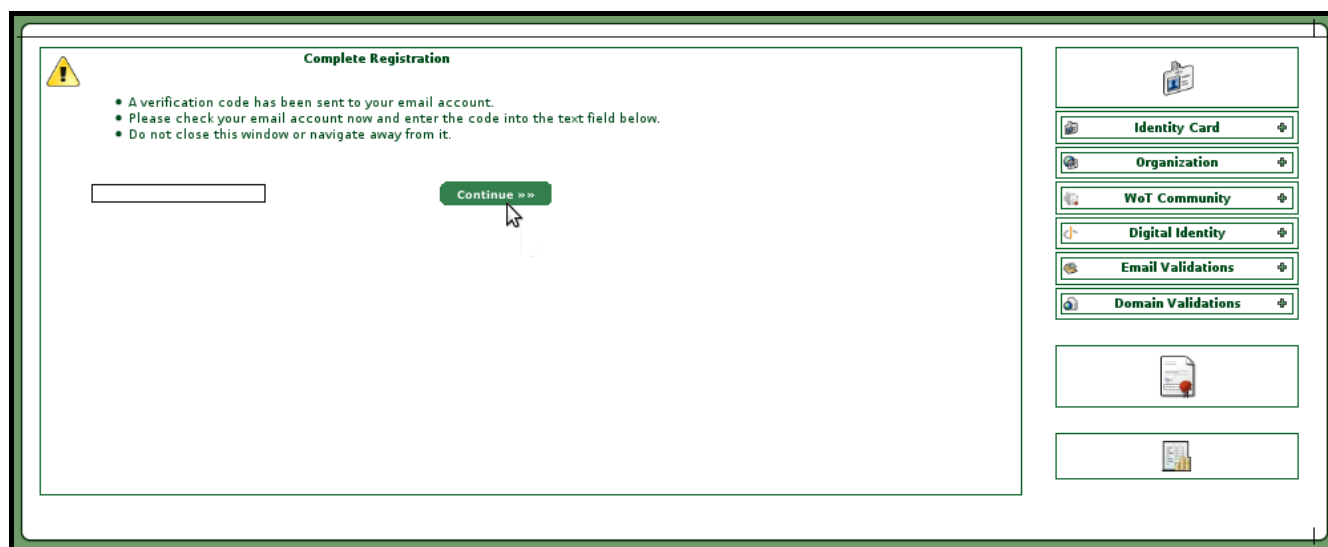
* Mail accounts from the following providers are not allowed: qq.com freemail.com rambler.ru mailnull.com laposte.fr yopmail.com

** Not seeing the States/Regions? Make sure you have JavaScript enabled.

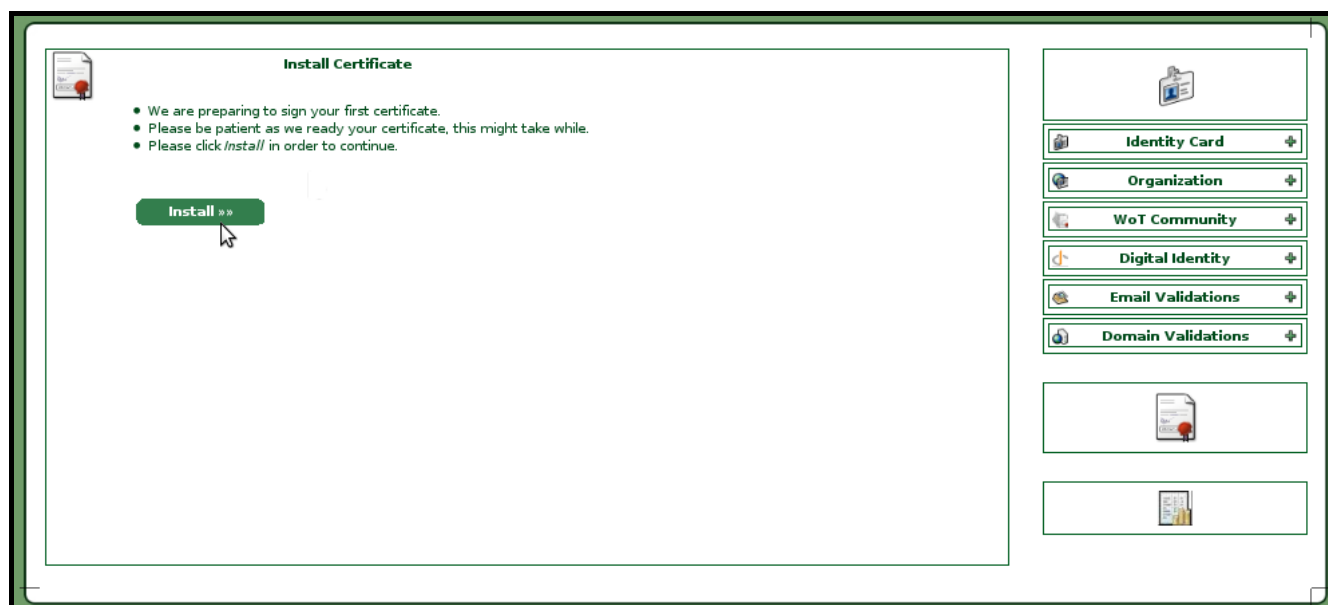
** States/Regions still missing of your country? Please help to improve it! **Send** a complete list to us.

Uwaga: Podczas rejestracji administrator musi podać prywatne dane osobowe. Bez nich nie będzie miał uprawnień do wygenerowania bezpłatnego certyfikatu oraz klucza.

6. W oknie, które się otworzy, kliknąć przycisk „OK”.
7. Sprawdzić skrzynkę mailową, której adres został podany podczas rejestracji. W otrzymanej wiadomości mailowej powinien znajdować się kod weryfikujący użytkownika, który należy wpisać w pustym polu. Kliknąć przycisk „Continue”.



8. W oknie informującym o generowaniu prywatnego klucza do osobistego certyfikatu użytkownika, potrzebnego do prawidłowej komunikacji ze stroną www.startssl.com, kliknąć przycisk „Continue”.
9. W celu zainstalowania osobistego certyfikatu należy kliknąć przycisk „Install”.

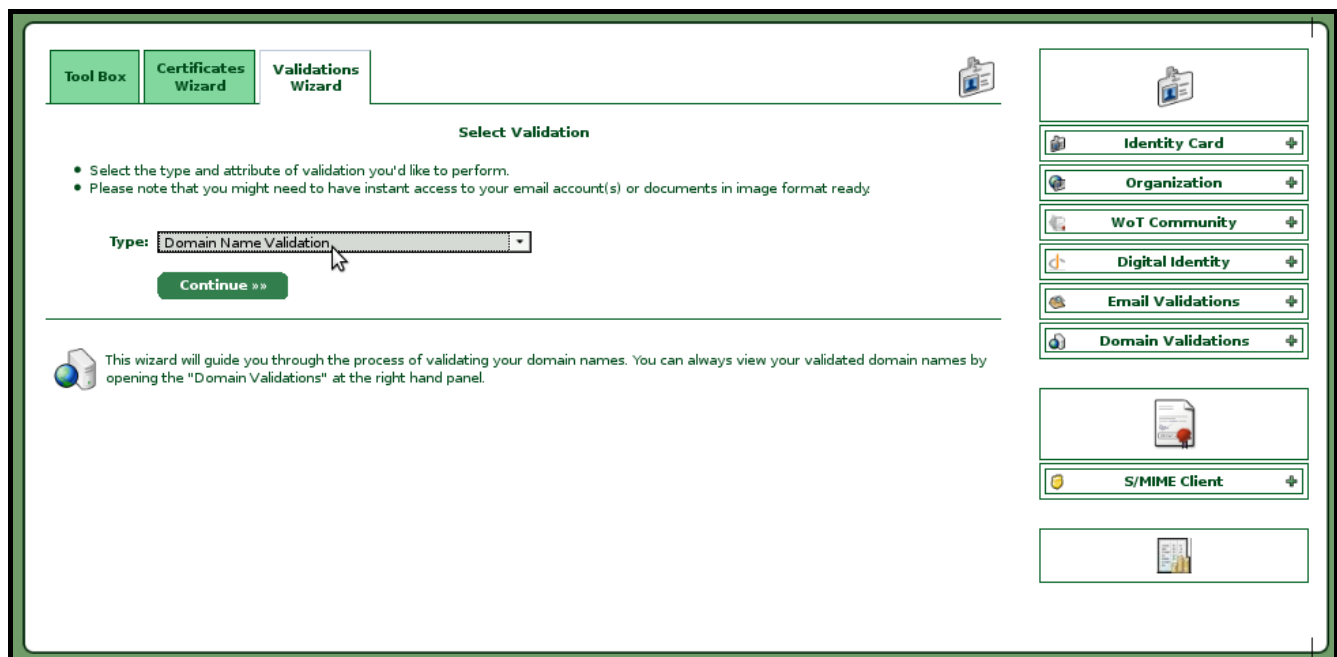


10. Certyfikat zostanie zainstalowany w przeglądarce internetowej na stałe. Zaleca się zachowanie jego kopii zapasowej. W tym celu należy zapoznać się z instrukcją „How do I backup my client certificates?” zamieszczoną w zakładce „F. A. Q.” na stronie <http://www.startssl.com/?app=25>. Kliknąć przycisk „Finish”.

11. Wyświetli się okno z zakładkami. Pozwolą one na przeprowadzenie weryfikacji właściciela domeny i na wygenerowanie certyfikatu ssl.crt oraz kodu ssl.key. Wybrać zakładkę „Validations Wizard”.



12. W celu uprawnomocnienia właściciela domeny, w polu „Type” z menu rozwijalnego wybrać opcję „Domain Name Validation” i kliknąć przycisk „Continue”.



13. W polu „http://” wpisać nazwę domeny. W polu obok wybrać właściwą domenę. Kliknąć przycisk „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 has the title 'Enter Domain Name' and two bullet points: 'Enter the domain name you want to have validated.' and 'You must be the owner of the top-level domain, sub domains are not supported.' Below this, there is a text input field containing 'http://stamview' and a dropdown menu showing '.pl'. A green 'Continue >>' button is positioned below the input field. On the right side, there is a sidebar with several expandable sections: 'Identity Card', 'Organization', 'WoT Community', 'Digital Identity', 'Email Validations', 'Domain Validations', 'S/MIME Client', and an empty section at the bottom.

14. Wybrać adres mailowy, na który zostanie wysłana wiadomość z kodem, który wykorzystywany jest w kolejnym kroku. W podanym przykładzie jest to adres „postmaster@stamview.pl”.

The screenshot shows the 'Select Verification Email' step of the SATEL installation wizard. The interface is similar to the previous step, with the same top navigation bar. The main content area has the title 'Select Verification Email' and a bullet point: 'Select the email address for verification of domain ownership from below.' Below this, there is a section labeled 'Verification Email:' with four radio button options: 'postmaster@stamview.pl' (which is selected), 'hostmaster@stamview.pl', 'webmaster@stamview.pl', and 'domeny@consultingservice.pl'. A green 'Continue >>' button is positioned below the options. On the right side, the sidebar is identical to the previous step.

15. W polu „Verification Code” wpisać kod otrzymany w wiadomości mailowej na wskazany w poprzednim oknie adres. Kliknąć przycisk „Continue”.

Complete Validation

- A verification code has been sent to "postmaster@stamview.pl".
- Please check your email account now and enter the code into the text field below.

Verification Code:

Continue >>

Identity Card

Organization

WoT Community

Digital Identity

Email Validations

Domain Validations

S/MIME Client

16. Kliknąć przycisk „Finish”.

Validation Success

- You have successfully authenticated domain "stamview.pl".
- You will be able to use this verification for the next 30 days, after which it expires and must be renewed.

Finish >>

Identity Card

Organization

WoT Community

Digital Identity

Email Validations

Domain Validations

S/MIME Client

17. Kliknąć na zakładkę „Certificates Wizard”. W polu „Certificate Target” wybrać opcję „Web Server SSL/TLS Certificate” i kliknąć przycisk „Continue”.

The screenshot shows the 'Certificates Wizard' window with the 'Certificates Wizard' tab selected. The title is 'Select Certificate Purpose'. It contains two bullet points: 'Make sure you have already validated a domain name or email address before using this tool! Select the "Validations Wizard" for this task.' and 'Depending on your preferences and type of software, you need to have a prepared certificate request (CSR) ready for submission.' Below this, the 'Certificate Target:' dropdown menu is set to 'Web Server SSL/TLS Certificate'. A 'Continue >>' button is highlighted with a mouse cursor. On the right side, there is a list of validation options: Identity Card, Organization, WoT Community, Digital Identity, Email Validations, and Domain Validations, each with a plus icon. Below this list are three more options: S/MIME Client and an empty box with a plus icon. At the bottom left, there is a small icon of a globe and a paragraph of text explaining that SSL/TLS web server certificates are used to secure communication and prevent eavesdropping, tampering, and message forgery.

18. W polu „Key password” wpisać hasło. Można wprowadzić od 10 do 32 znaków (cyfry i litery). W polu „Confirm Password” potwierdzić hasło, wpisując je ponownie. Kliknąć przycisk „Continue”.

The screenshot shows the 'Certificates Wizard' window with the 'Certificates Wizard' tab selected. The title is 'Generate Private Key'. It contains three bullet points: 'If you created your own private key and certificate request (CSR), please skip this step.', 'Provide a password for your private key (At least 10 characters, max. 32)', and 'Allowed are only letters and numbers, without spaces!'. Below this, there are two password fields: 'Key Password:' and 'Confirm Password:', both filled with dots. A 'Keysize:' dropdown menu is set to '2048 (Medium)'. 'Skip >>' and 'Continue >>' buttons are at the bottom. A mouse cursor is pointing at the 'Continue >>' button. On the right side, the same list of validation options as in the previous screenshot is visible. At the bottom left, there is a small icon of a key and a paragraph of text explaining that at this step a private key is generated for the certificate and it can only be used with the corresponding private key.

19. Zaznaczyć i skopiować (Ctrl+C) tekst, który pojawi się w polu tekstowym. Otworzyć „Notatnik” i wkleić skopiowany tekst. Zapisać plik jako „ssl.key”. Kliknąć przycisk „Continue”.

The screenshot shows the 'Save Private Key' step of the 'Certificates Wizard'. The interface includes a 'Tool Box' tab, a 'Certificates Wizard' tab, and a 'Validations Wizard' tab. The main content area contains instructions and a text box with a private key. The instructions are:

- Copy and paste the content from the textbox below into a file and save it as **ssl.key**.
- Make sure, that you do not alter the content and you did not add any spaces! Save it in ASCII format (plain text).
- Allowed are only letters and numbers, without spaces!
- Decrypt the private key with the OpenSSL utility: **openssl rsa -in ssl.key -out ssl.key** or use the utility from the Tool Box.

The text box contains the following text:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,9AF3777FAEB4A1955B6DB93EEC7CE4DB
OTaMCdmbWwQuCXom+meJ/q4G00QuUDu9Kj2y8t0R4eV/G18uE9bJ/Mrxyx4OARv6
BkS9A6eGUwCpQadu/tNK2PrMfNU7wegD+seoqo40IjmubbbubWbfcgGPR/jspo1G
bd cUKQ1kPRxQ4MD540yLk8LUMsQnuN8Tdt0QSxjmK9KauLi8AvKnogRL7xJJNI4
-----
```

Below the text box is a 'Continue >>' button. On the right side of the window, there is a sidebar with several icons and labels: 'Identity Card', 'Organization', 'WoT Community', 'Digital Identity', 'Email Validations', 'Domain Validations', 'S/MIME Client', and a folder icon.

20. W oknie, które się otworzy, wybrać nazwę zweryfikowanej wcześniej domeny. Kliknąć przycisk „Continue”.

The screenshot shows the 'Add Domains' step of the 'Certificates Wizard'. The interface includes a 'Tool Box' tab, a 'Certificates Wizard' tab, and a 'Validations Wizard' tab. The main content area contains instructions and a dropdown menu for selecting a domain. The instructions are:

- Select the top target domain name for your certificate.
- Note: Only domain names which were validated within the last 30 days are eligible for selection.

The domain selection dropdown is labeled 'Domain:' and shows 'stamview.pl' as the selected option. Below the dropdown is a 'Continue >>' button. On the right side of the window, there is a sidebar with several icons and labels: 'Identity Card', 'Organization', 'WoT Community', 'Digital Identity', 'Email Validations', 'Domain Validations', 'S/MIME Client', and a folder icon.

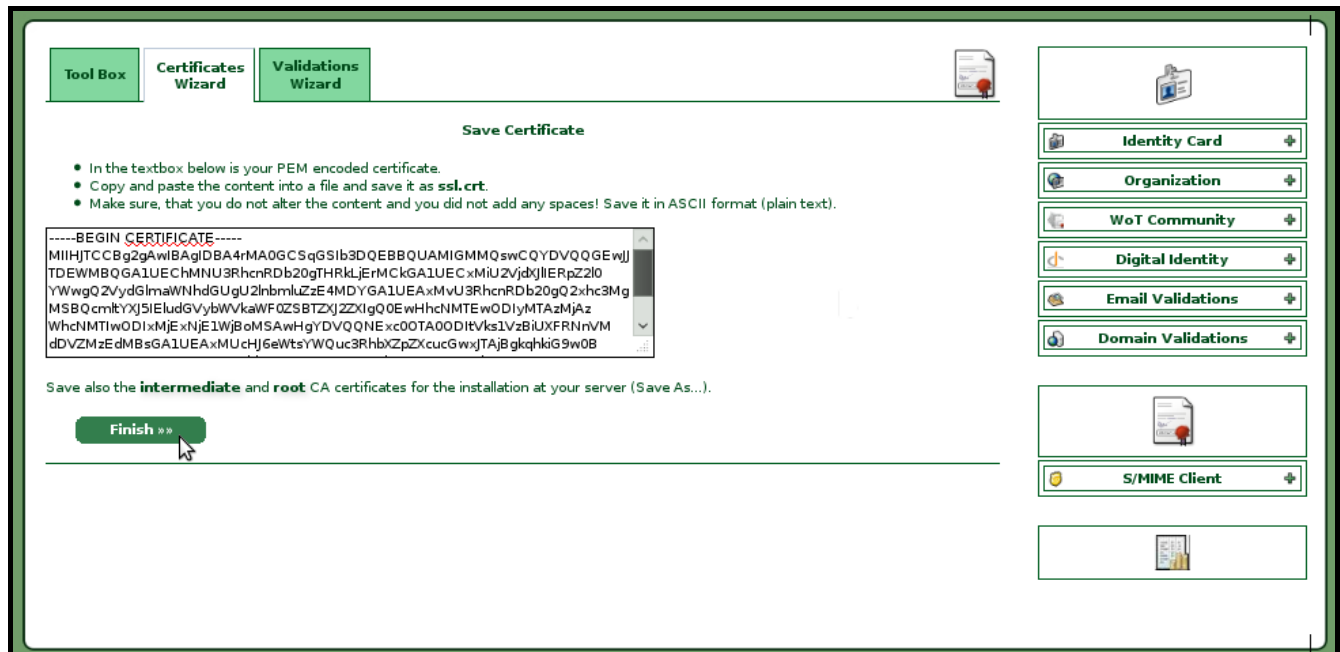
21. Utworzyć poddomenę w ramach zweryfikowanej wcześniej domeny. Będzie to adres systemu STAM-VIEW, do którego będą się logować użytkownicy. W oknie poniżej został podany przykładowy adres <http://przyklad.stamview.pl>. Kliknąć przycisk „Continue”.

The screenshot shows the 'Add Domains' step of the 'Certificates Wizard'. The interface includes a top navigation bar with 'Tool Box', 'Certificates Wizard', and 'Validations Wizard'. The main content area has a title 'Add Domains' and a list of instructions: '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".'. Below the instructions, there is a text input field containing 'http://przyklad.stamview.pl' and a green 'Continue >>' button. On the right side, there is a sidebar with a list of validation steps: 'Identity Card', 'Organization', 'WoT Community', 'Digital Identity', 'Email Validations', and 'Domain Validations', each with a plus icon. Below this list, there are sections for 'S/MIME Client' and a document icon.

22. Zostanie wygenerowany jeden certyfikat o nazwie, w tym przypadku – „przyklad.stamview.pl”, wspólny dla domeny oraz poddomeny. Kliknąć przycisk „Continue”.

The screenshot shows the 'Ready Processing Certificate' step of the 'Certificates Wizard'. The interface is similar to the previous step, with the same top navigation bar. The main content area has a title 'Ready Processing Certificate' and a list of instructions: '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.'. Below the instructions, there is a green 'Continue >>' button. On the right side, the sidebar is identical to the previous step, showing the same list of validation steps and sections for 'S/MIME Client' and a document icon.

23. Zaznaczyć i skopiować (Ctrl+C) tekst, który pojawi się w polu tekstowym. Otworzyć „Notatnik” i wkleić skopiowany tekst. Zapisać plik jako „ssl.crt”. Kliknąć przycisk „Finish”. Pliki „ssl.key” oraz „ssl.crt” są przygotowane do wgrania ich do systemu STAM-VIEW.



3.1.1 Odkodowanie pliku „ssl.key”

Plik „ssl.key” jest zakodowany hasłem. Jeżeli zostanie w takiej formie, podczas wgrywania certyfikatów do systemu STAM-VIEW, będzie trzeba podać w odpowiednim polu hasło. Można go też rozkodować w programie generującym certyfikaty, od razu po zapisaniu pliku „ssl.crt”.

W celu odkodowania pliku „ssl.key” w programie generującym certyfikaty, administrator powinien wykonać następujące czynności:

1. Wybrać zakładkę „Tool Box”.
2. Zaznaczyć opcję „Decrypt Private Key”.
3. W pliku „ssl.key” zaznaczyć cały tekst, skopiować go i wkleić w pole tekstowe, które się wyświetliło w oknie.
4. W polu „Key password” wpisać hasło, które było podawane przy generowaniu pliku „ssl.key” (patrz: punkt 18 z poprzedniego rozdziału) i kliknąć przycisk „Decrypt”.
5. Zaznaczyć i skopiować (Ctrl+C) odkodowany tekst, który pojawi się w polu tekstowym. Otworzyć „Notatnik” i wkleić skopiowany tekst. Zapisać plik jako „ssl.key” zastępując nim poprzednio zapisany plik o tej samej nazwie.

Uwaga: Darmowe certyfikaty zwykle są generowane na określony okres czasu. Należy pamiętać, żeby w odpowiednim momencie wygenerować je ponownie.

3.2 Certyfikaty innych jednostek certyfikujących

Istnieje możliwość korzystania z certyfikatów innych jednostek certyfikujących. W takim przypadku, postępując zgodnie z poleceniami poszczególnych jednostek, administrator musi wygenerować pliki odpowiednich certyfikatów, zapisać je na dysku i wgrać do systemu STAM-VIEW.

4. Zarządzanie systemem

System współpracuje z przeglądarkami Mozilla Firefox (zalecana), Google Chrome oraz Internet Explorer od wersji 8.0.

Uwaga: Brak aktywności przez 10 minut powoduje wylogowanie z systemu. Każde kliknięcie w celu wybrania innej zakładki, skutkuje odliczaniem czasu na nowo.

4.1 Pierwsze logowanie

1. Na komputerze podłączonym do sieci lokalnej, do której jest podłączony serwer VMWare ESXi, wpisać w przeglądarce internetowej adres: **http://[adres wirtualnej maszyny STAM-VIEW]**. Adres może zostać wprowadzony w formie adresu IP (4 liczby dziesiętne oddzielone kropkami) lub w postaci nazwy domeny.
2. Zalogować się do systemu (wpisać login, hasło i kod z obrazka). W systemie fabrycznie dla administratora zaprogramowane są login **Administrator** oraz hasło **satel**.



3. Wejść do zakładki „Ustawienia”, a w niej wybrać zakładkę „Certyfikaty SSL”.
4. W przypadku wygenerowania certyfikatów SSL firmy StartCom, należy w polu „Plik certyfikatu (*.crt)” kliknąć przycisk „Przeglądaj...” i wybrać zapisany wcześniej plik „ssl.crt”. W polu „Plik klucza (*.key)” kliknąć przycisk „Przeglądaj...” i wybrać zapisany wcześniej plik „ssl.key”. Jeżeli plik klucza jest nadal zakodowany, w polu „Hasło klucza (jeżeli zakodowany)”, wpisać hasło, które było podawane przy generowaniu pliku „ssl.key” (patrz: instrukcja instalacji systemu). Kliknąć przycisk „Wyślij”.
5. W przypadku wygenerowania certyfikatów SSL innej jednostki certyfikującej, należy w polu „Plik CA” kliknąć przycisk „Przeglądaj...” i wybrać odpowiedni plik. W polu „Plik łańcucha certyfikatu” kliknąć przycisk „Przeglądaj...” i wybrać odpowiedni plik. Kliknąć przycisk „Wyślij”.

6. Po zaakceptowaniu certyfikatu oraz klucza, status certyfikatów SSL / jednostki autoryzującej w obu polach zmieni się na „OK”.

The screenshot shows the Stam-View web interface. At the top, there is a header with the Satel logo, the title 'Stam-View – system zdalnego dostępu do stacji monitorującej STAM-2', the date and time '13-09-2011 12:32', and the language 'EN PL'. Below the header, there is a navigation menu on the left with options like 'Dodaj użytkownika', 'Pokaż użytkowników', 'Lista zdarzeń', 'Wiadomości', 'Ustawienia', 'Logi', 'Kopie zapasowe', and 'Aktualizacja'. The main content area is titled 'Ustawienia' and contains several tabs: 'Hasło', 'Logo', 'Użytkownicy', 'Instalatorzy', 'Certyfikaty SSL', and 'Języki'. The 'Certyfikaty SSL' tab is selected. It contains two sections: 'Status certyfikatów SSL' and 'Certyfikaty jednostki autoryzującej'. The 'Status certyfikatów SSL' section has two rows: 'Plik certyfikatu (*.crt):' and 'Plik klucza (*.key):', both with the value 'Domyślny (wymagana zmiana)'. The 'Certyfikaty jednostki autoryzującej' section has two rows: 'Plik CA:' and 'Plik łańcucha certyfikatu:', both with the value 'StartSSL'. Below these sections, there are two 'Wyślij certyfikaty' sections. Each section has three rows: 'Plik certyfikatu (*.crt):', 'Plik klucza (*.key):', and 'Hasło klucza (jeżeli zakodowany):'. Each row has a text input field and a 'Przeglądaj...' button. At the bottom of each section is a 'Wyślij' button.

4.2 Kolejne logowania

W celu uzyskania dostępu do systemu STAM-VIEW należy wpisać w przeglądarce następujący adres: **https://[adres wirtualnej maszyny STAM-VIEW]**. Adres może zostać wprowadzony w formie adresu IP (4 liczby dziesiętne oddzielone kropkami) lub w postaci nazwy domeny.

4.3 Zmiana hasła

Hasło fabryczne należy zmienić po pierwszym zalogowaniu się do systemu. Administrator, w celu zmiany hasła, powinien wykonać następujące czynności:

1. Wybrać zakładkę „Ustawienia”.
2. Kliknąć zakładkę „Hasło”.

3. Wpisać najpierw stare hasło, potem nowe. Następnie powtórzyć je w kolejnym polu. Zatwierdzić wprowadzoną zmianę przyciskiem „Zmień hasło”.

4.4 Informacje wyświetlane po zalogowaniu się do systemu

The screenshot displays the Stam-View web interface. At the top, the Satel logo is on the left, and the title 'Stam-View – system zdalnego dostępu do stacji monitorującej STAM-2' is in the center. The top right corner shows the date '09-08-2011 08:29' and language options 'PL EN RU'. Below the title bar, a navigation menu on the left lists: 'Dodaj użytkownika', 'Pokaż użytkowników', 'Lista zdarzeń', 'Wiadomości', 'Ustawienia', 'Logi', 'Kopie zapasowe', and 'Aktualizacja'. The main content area shows the user 'Witaj, Administrator' and the last login time 'Ostatnie logowanie: 2011-08-08 08:34:21, Nieudane: 2011-07-29 12:18:59'. A 'Wyloguj' button is in the top right. The main heading is 'System zdalnego dostępu do stacji monitorującej STAM-2'. Below it, two status indicators show 'Liczba nieprzeczytanych wiadomości: 0' and 'Liczba zdarzeń od ostatniej wizyty: 0'. A 'Status' section contains a table with three rows: 'Wersja Stam-View' (OK), 'Rejestracja w STAM-2' (OK), and 'Certyfikaty SSL' (OK). A 'Wersja' section shows 'Wersja 27072011 (BETA)'.

Status	
Wersja Stam-View	OK
Rejestracja w STAM-2	OK
Certyfikaty SSL	OK

Wersja	
Wersja	27072011 (BETA)

Po każdym zalogowaniu się do systemu, w oknie wyświetlają się informacje dotyczące: czasu ostatniego udanego i nieudanego logowania, nieprzeczytanych wiadomości, liczby zdarzeń, które zostały odebrane przez stację monitorującą od ostatniego logowania oraz wersja oprogramowania, status komunikacji pomiędzy systemem STAM-VIEW a stacją monitorującą i status certyfikatów SSL. W przypadku jakichkolwiek niezgodności przy każdym ze statusów pojawiają się informacje w czerwonym kolorze.

Jeżeli przy polu "Wersja Stam-View" pojawi się czerwony komunikat „Wymaga aktualizacji”, administrator systemu powinien zaktualizować wersję STAM-VIEW. Ze strony www.satel.pl należy pobrać odpowiedni plik z aktualizacją i zapisać go na dysku. Następnie wybrać zakładkę „Aktualizacja”, a w niej kliknąć polecenie „Kliknij tutaj, aby zaktualizować”. W polu „Plik z aktualizacją” podać ścieżkę dostępu do pobranego pliku.

Jeżeli przy polu „Rejestracja w STAM-2” wyświetli się czerwony komunikat „Brak”, należy skonfigurować połączenie systemu STAM-VIEW ze stacją monitorującą. W tym celu operator stacji monitorującej powinien w programie STAM-2 w oknie „Konfiguracja” w zakładce „Ustawienia” zaznaczyć opcję „Włączony”, wypełnić prawidłowo pola konieczne do prawidłowego połączenia i kliknąć przycisk „Zastosuj”. Następnie zamknąć program STAM-2 Serwer i uruchomić go ponownie. Gdy system STAM-VIEW odbierze dane od stacji monitorującej, w oknie wyświetli się komunikat „OK”.

Jeżeli przy polu „Certyfikaty SSL” wyświetli się czerwony komunikat „Brak”, należy ponownie wgrać do systemu STAM-VIEW certyfikaty. Administrator powinien wybrać zakładkę

„Ustawienia”, a w niej zakładkę „Certyfikaty SSL”. Przy certyfikatach SSL oraz jednostki autoryzującej będzie się wyświetlał czerwony komunikat „Brak”. Należy wgrać przy pomocy przycisku „Wyślij” odpowiednie pliki z certyfikatami.

4.5 Zmiana logo

Istnieje możliwość podmiany logo wyświetlanego w górnej części okna systemu. W tym celu administrator powinien wykonać następujące czynności:

1. Zalogować się do systemu.
2. Wybrać zakładkę „Ustawienia”, a w niej zakładkę „Logo”.
3. Kliknąć na przycisk „Przeglądaj” i wybrać plik z przygotowanym wcześniej logo.

Uwaga: System akceptuje tylko pliki typu: PNG, BMP i GIF o rozdzielczości 200 x 74 pikseli.

4. Kliknąć przycisk „Zmień logo”.
5. Określić położenie obrazka, wyrównując go w poziomie i pionie przy pomocy odpowiednich przycisków.

4.6 Uprawnienia administratora w systemie

1. Dodawanie, edytowanie oraz usuwanie użytkowników (hasła mogą liczyć od 4 do 16 znaków).
2. Przydzielanie uprawnień użytkownikom.

The screenshot displays the Stam-View web interface. At the top, the Satel logo is on the left, and the title 'Stam-View – system zdalnego dostępu do stacji monitorującej STAM-2' is in the center. The top right corner shows the date and time '29-07-2011 12:07' and language options 'PL EN RU'. Below the title bar, a navigation menu on the left lists various functions: 'Dodaj użytkownika', 'Pokaż użytkowników', 'Lista zdarzeń', 'Wiadomości', 'Ustawienia', 'Logi', 'Kopie zapasowe', and 'Aktualizacja'. The main content area is titled 'Podaj dane nowego użytkownika' and contains several input fields: 'Instalator' with a checkbox, 'Login:', 'Hasło:', 'Powtórz hasło:', 'Lista abonentów (obiektów):' with the value 'Brak', and 'Obiekt:' with a dropdown menu. A 'Wyloguj' button is visible in the top right, and a 'Dodaj użytkownika' button is at the bottom of the form.

3. Możliwość wyszukiwania użytkowników według nazwy.



Stam-View – system zdalnego dostępu
do stacji monitorującej STAM-2

18-08-2011 11:10
PL EN RU

9:56 [Wyloguj](#)

[Dodaj użytkownika](#)
[Pokaż użytkowników](#)
[Lista zdarzeń](#)
[Wiadomości](#)
[Ustawienia](#)
[Logi](#)
[Kopie zapasowe](#)
[Aktualizacja](#)

Witaj, Administrator

Ostatnie logowanie: 2011-08-18 08:42:08, Nieudane: 2011-08-17 15:49:54

Lista zarejestrowanych użytkowników

 Szukaj użytkownika

Użytkownik	Typ użytkownika	Akcje
Administrator	Administrator	
Juszczak R	Instalator	 
Kowalski J	Użytkownik	 
Kwiatkowska M	Instalator	 
Kwiecień E	Użytkownik	 
Nowak S	Użytkownik	 
Penderecki K	Użytkownik	 
Sowiński H	Użytkownik	 
Wenda K	Instalator	 

Wyników na stronie 10 ▼

4. Filtrowanie zdarzeń zgodnie z następującymi kryteriami:
- wszystkie lub wybrane,
 - dotyczące wybranego okresu czasu,
 - dotyczące wybranego abonenta (o określonym loginie, numerze ID lub nazwie) lub wszystkich,
 - zawierające wpisany tekst,
 - z potwierdzeniem obrazu wideo.



Stam-View – system zdalnego dostępu
do stacji monitorującej STAM-2

09-11-2011 14:17

EN PL RU

9:45 [Wyloguj](#)

Dodaj użytkownika

Pokaż użytkowników

Lista zdarzeń

Wiadomości

Ustawienia

Logi

Kopie zapasowe

Aktualizacja

Witaj, **Administrator**

Ostatnie logowanie: 2011-11-08 12:33:16, Nieudane: 2011-10-27 19:53:54

Lista zdarzeń

🔍 Zmień parametry filtra

Data	Typ	Informacje	Wideo
2011-10-28 07:28:31	Alarm	Włamanie	
2011-10-28 07:28:06	Test	Okresowa transmisja ...	
2011-10-28 07:24:07	Uwaga	Restart systemu	
2011-10-28 07:21:43	Alarm	Włamanie	
2011-10-28 06:53:59	Uwaga	Kod nieznany - brak ...	
2011-10-28 06:48:04	Info	Wejście do konfigurac...	
2011-10-28 06:48:02	Alarm	Potrzebna pomoc medy...	
2011-10-28 06:47:52	Alarm	Alarm pożarowy	
2011-10-27 23:27:48	Uwaga	Restart systemu	
2011-10-27 23:04:06	Info	Wejście do konfigurac...	

strona 1 z 8971 następna >>

Wyników na stronie

5. Przeglądanie szczegółowe zdarzeń.

6. Możliwość komunikacji z instalatorami oraz użytkownikami przy pomocy systemu wiadomości.

Satel

Stam-View – system zdalnego dostępu
do stacji monitorującej STAM-2

18-08-2011 11:51
PL EN RU

6:52 **Wyloguj**

Dodaj użytkownika

Pokaż użytkowników

Lista zdarzeń

Wiadomości

Ustawienia

Logi

Kopie zapasowe

Aktualizacja

Witaj, Administrator

Ostatnie logowanie: 2011-08-18 09:48:24, Nieudane: 2011-08-17 15:49:54

Wiadomości

Odebrane

Wysłane

Napisz

Do:

Kowalski J

Wszyscy

Treść:

Witam

Zgodnie z ustaleniami kwota ostatniej faktury zostanie obniżona o 10%. Faktura korygująca do odbioru w księgowości.

Wyślij wiadomość

7. Konfiguracja ustawień systemu STAM-VIEW:

- możliwość zmiany hasła,
- możliwość podmiany logo wyświetlanego w górnej części okna systemu (domyślnie jest tam wyświetlane logo firmy SATEL),
- definiowanie uprawnień dla wszystkich użytkowników,
- definiowanie uprawnień dla wszystkich instalatorów,
- wgrywanie certyfikatów SSL,
- wybór trzech języków, z których będą mogli korzystać użytkownicy systemu,
- wybór domyślnego języka dla wszystkich użytkowników.



Stam-View – system zdalnego dostępu
do stacji monitorującej STAM-2

13-09-2011 13:39
DE EN PL

9:51 **Wyloguj**

Dodaj użytkownika

Pokaż użytkowników

Lista zdarzeń

Wiadomości

Ustawienia

Logi

Kopie zapasowe

Aktualizacja

Witaj, **Administrator**

Ostatnie logowanie: 2011-09-13 13:16:13, Nieudane: 2011-09-13 12:24:30

Ustawienia

Hasło

Logo

Użytkownicy

Instalatorzy

Certyfikaty SSL

Języki

Może usuwać wiadomości

☒

Typy zdarzeń

☒ Alarm

☒ Wyłączenie czuwania

☒ Test

☐ Info

☒ Fałszywy alarm

☐ Zalogowanie

☐ SMS

☒ Włączenie czuwania

☒ Awaria

☒ Uwaga

☐ Komentarz

☒ Niepoprawne wył. Czuwania

☐ Wylogowanie

☐ Telefon

Zapisz

8. Możliwość wykonywania kopii zapasowych ustawień systemu STAM-VIEW, ich zapisywania na dysku, w bazie systemu STAM-VIEW oraz przywracania zapisanej konfiguracji systemu.



Stam-View – system zdalnego dostępu
do stacji monitorującej STAM-2

29-07-2011 12:23
PL EN RU

9:44 [Wyloguj](#)

[Dodaj użytkownika](#)
[Pokaż użytkowników](#)
[Lista zdarzeń](#)
[Wiadomości](#)
[Ustawienia](#)
[Logi](#)
[Kopie zapasowe](#)
[Aktualizacja](#)

Witaj, Administrator

Ostatnie logowanie: 2011-07-29 11:17:18, Nieudane: 2011-07-29 12:06:53

Kopie zapasowe

[Kopie](#) [Wyślij](#)

Dostępne kopie zapasowe

Data wykonania	Akcje
2011-07-28 11:08:43	🗑 ↕ ⬆

[Wykonaj nową](#)

9. Przeglądanie zdarzeń systemowych dotyczących STAM-VIEW.



Stam-View – system zdalnego dostępu
do stacji monitorującej STAM-2

18-08-2011 11:09
PL EN RU

9:50 [Wyloguj](#)

[Dodaj użytkownika](#)
[Pokaż użytkowników](#)
[Lista zdarzeń](#)
[Wiadomości](#)
[Ustawienia](#)
[Logi](#)
[Kopie zapasowe](#)
[Aktualizacja](#)

Witaj, Administrator

Ostatnie logowanie: 2011-08-18 08:42:08, Nieudane: 2011-08-17 15:49:54

Logi systemowe

Data	Akcja	Opis
2011-08-18 09:07:54	Przypisanie obiektu	Obiekt: 14 Do: Wenda K
2011-08-18 09:07:54	Przypisanie obiektu	Obiekt: 12 Do: Wenda K
2011-08-18 09:07:54	Dodanie użytkownika	Wenda K
2011-08-18 09:07:06	Przypisanie obiektu	Obiekt: 13 Do: Sowiński H
2011-08-18 09:07:06	Dodanie użytkownika	Sowiński H
2011-08-18 09:06:36	Przypisanie obiektu	Obiekt: 1 Do: Kowalski J
2011-08-18 09:06:36	Dodanie użytkownika	Kowalski J
2011-08-18 09:06:05	Dodanie użytkownika	Kwiecień E
2011-08-18 09:06:05	Przypisanie obiektu	Obiekt: 12 Do: Kwiecień E
2011-08-18 09:04:52	Przypisanie obiektu	Obiekt: 13 Do: Juszczak R

strona 1 z 36

Wyników na stronie

[następna >>](#)

10. Aktualizacja wersji oprogramowania systemu STAM-VIEW.



Stam-View – system zdalnego dostępu
do stacji monitorującej STAM-2

29-07-2011 12:23
PL EN RU
9:54 [Wyloguj](#)

[Dodaj użytkownika](#)
[Pokaż użytkowników](#)
[Lista zdarzeń](#)
[Wiadomości](#)
[Ustawienia](#)
[Logi](#)
[Kopie zapasowe](#)
[Aktualizacja](#)

Witaj, **Administrator**
Ostatnie logowanie: 2011-07-29 11:17:18, **Nieudane:** 2011-07-29 12:06:53

Aktualizacja

Zainstalowana wersja interfejsu www: **28072011**

[Kliknij tutaj aby zaktualizować](#)