



**PROGRAM
REGIONALNY**
NARODOWA STRATEGIA SPÓJNOŚCI



Małopolska

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO



MAŁOPOLSKA KARTA AGLOMERACYJNA — SYSTEM ZARZĄDZANIA TRANSPORTEM ZBIOROWYM W WOJEWÓDZTWIE MAŁOPOLSKIM

CZĘŚĆ I — BUDOWA SYSTEMU ZARZĄDZANIA TRANSPORTEM ZBIOROWYM NA TERENIE WOJEWÓDZTWA MAŁOPOLSKIEGO

PROCEDURY EKSPLOATACYJNE



Historia zmian				
Wersja	Data	Opis	Autor	Uwagi
0.1	2015-01-01			
0.2				
0.3				

Spis treści

1. OPIS OGÓLNY	5
2. PROCEDURY ADMINISTRACYJNE	5
2.1. Wstęp	6
2.2. Ładowanie aplikacji SmartCity na klaster aplikacyjny	6
2.3. Procedura konfiguracji stacji POK	7
2.3.1. Wstęp	8
2.3.2. Oprogramowanie	8
2.3.3. Certyfikat	17
2.3.4. Konfiguracja SmartCity	20
3. PROCEDURY AWARYJNE	21
3.1. Wstęp	22
3.2. Procedura awaryjnego przełączenia systemu MKA do zapasowej serwerowni CPD2.	22
3.3. Procedura uruchomienia środowiska CPD1 lub CPD2	23
3.3.1. Wstęp	24
3.3.2. Kroki procedury	24
4. PROCEDURY BACKUPU	26
4.1. Wstęp	27
4.2. Definicje pojęć	27
4.3. Informacje ogólne o systemie tworzenia kopii bezpieczeństwa	27
4.4. Odtwarzanie danych z kopii bezpieczeństwa	27
4.5. Polityka kopii bezpieczeństwa	28

Historia zmian

Wersja	Data	Opis	Autor	Uwagi
0.1	2015-11-04	Utworzenie	Atos	

1. Opis ogólny

Niniejsza dokumentacja stanowi część dokumentacji eksploatacyjnej. Procedury eksploatacyjne to zestaw dokumentów zawierających opisy przeznaczone dla administratorów Systemu MKA, którzy będą w zakresie swoich obowiązków służbowych dbać o prawidłowe funkcjonowanie System MKA.

W ramach procedur eksploatacyjnych przygotowano następujące dokumenty:

2. Procedury administracyjne

Historia zmian

Wersja	Data	Opis	Autor	Uwagi
0.1	2015-11-04	Utworzenie	Atos	

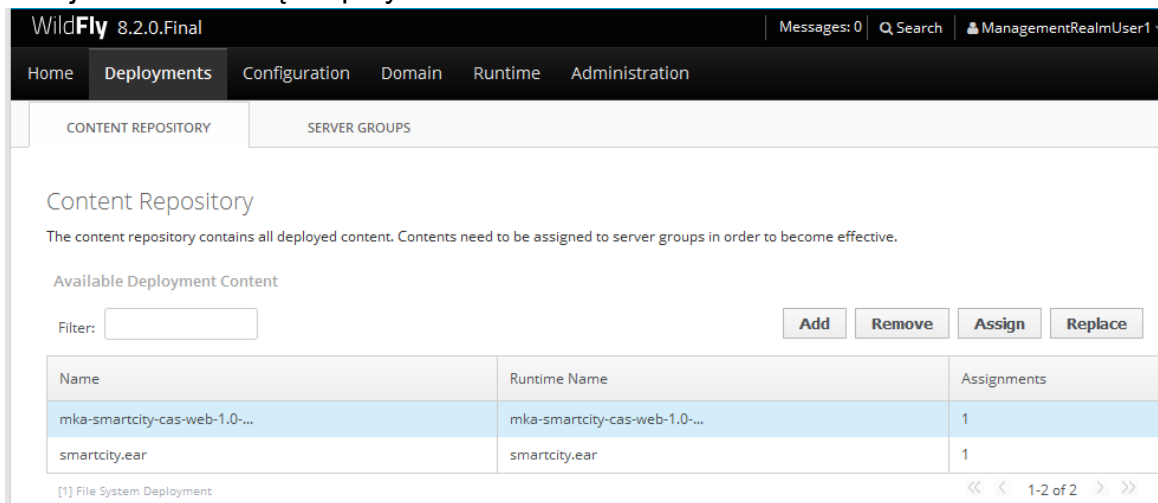
2.1. Wstęp

Niniejsza dokumentacja stanowi zbiór Procedur administracyjnych. Zawiera informacje przeznaczone dla administratorów, którzy w ramach swoich obowiązków służbowych będą odpowiedzialni za instalację, uruchomienie i utrzymanie systemów i urządzeń stanowiących elementy systemu MKA. Procedury administracyjne obejmują następujące obszary:

- [Instalacja SmartCity](#)
- [Procedura konfiguracji stacji POK](#)

2.2. Ładowanie aplikacji SmartCity na klaster aplikacyjny

1. Zaloguj się do VPN MKA
2. Otwórz przeglądarkę z adresem XXXXXXXXXX dla CPD1 lub YYYYYYYYYYYY dla CPD2.
3. Zaloguj się do konsoli systemowej JBoss Wildfly
4. Przejdź na zakładkę Deployments



WildFly 8.2.0.Final | Messages: 0 | Search | ManagementRealmUser1

Home | **Deployments** | Configuration | Domain | Runtime | Administration

CONTENT REPOSITORY | SERVER GROUPS

Content Repository

The content repository contains all deployed content. Contents need to be assigned to server groups in order to become effective.

Available Deployment Content

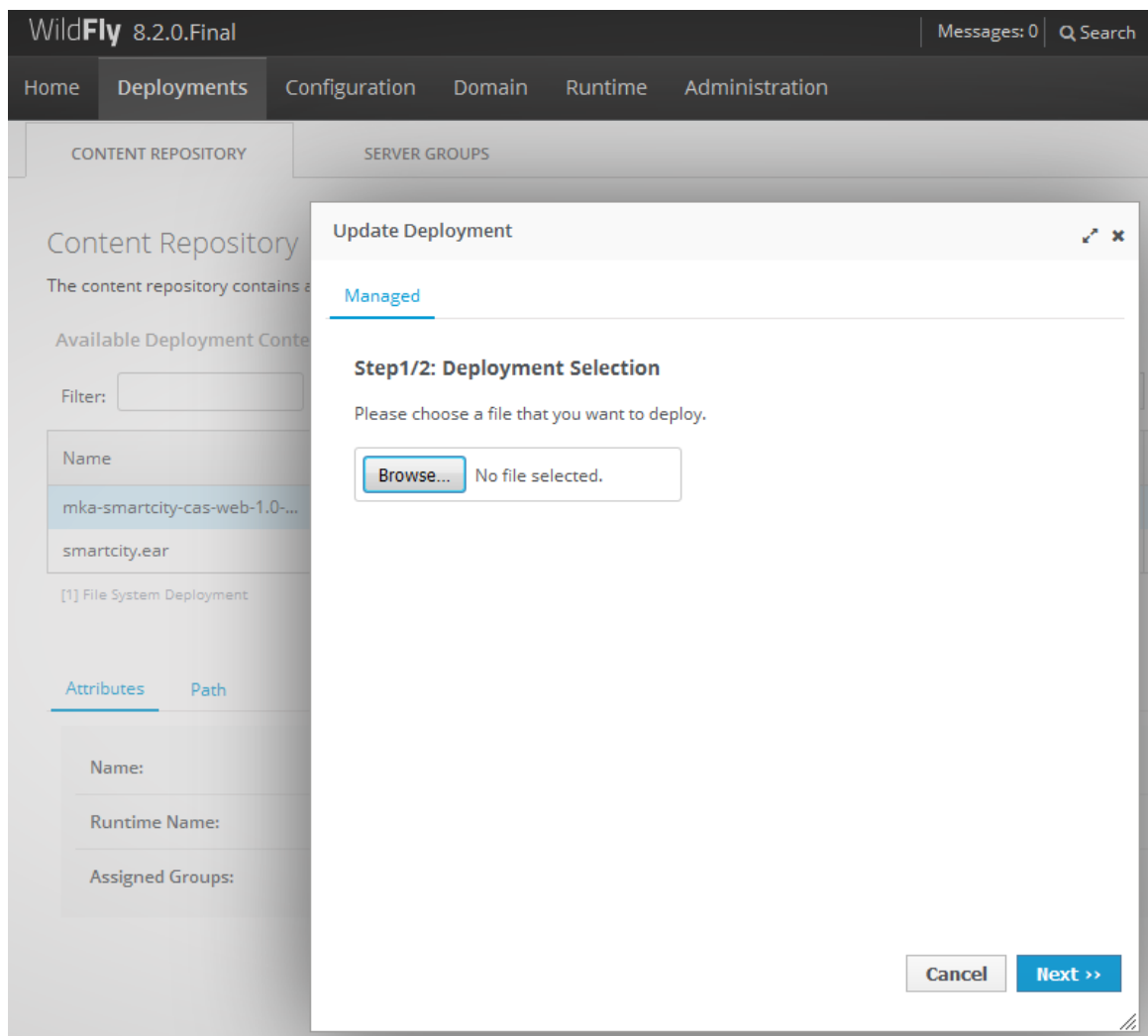
Filter:

Add Remove Assign Replace

Name	Runtime Name	Assignments
mka-smartcity-cas-web-1.0-...	mka-smartcity-cas-web-1.0-...	1
smartcity.ear	smartcity.ear	1

[1] File System Deployment | 1-2 of 2

5. Zaznacz smartcity.ear i wciśnij guzik Replace
6. Wciśnij przycisk Browse i znajdź nowy pakiet .ear na dysku lokalnym
7. Wciśnij OK



8. Poczekaj na załadowanie nowej wersji EAR

2.3. Procedura konfiguracji stacji POK

Historia zmian

Wersja	Data	Opis	Autor	Uwagi
0.1	2015-11-04	Utworzenie	Atos	



2.3.1. Wstęp

Niniejsza dokument stanowi część dokumentacji Procedur administracyjnych. Dokument zawiera informacje przeznaczone dla administratorów, którzy w ramach swoich obowiązków służbowych będą odpowiedzialni za instalację, uruchomienie i utrzymanie stacji roboczych w POK MKA.

2.3.2. Oprogramowanie

2.3.2.1. Przeglądarka Firefox

2.3.2.1.1. Wersja

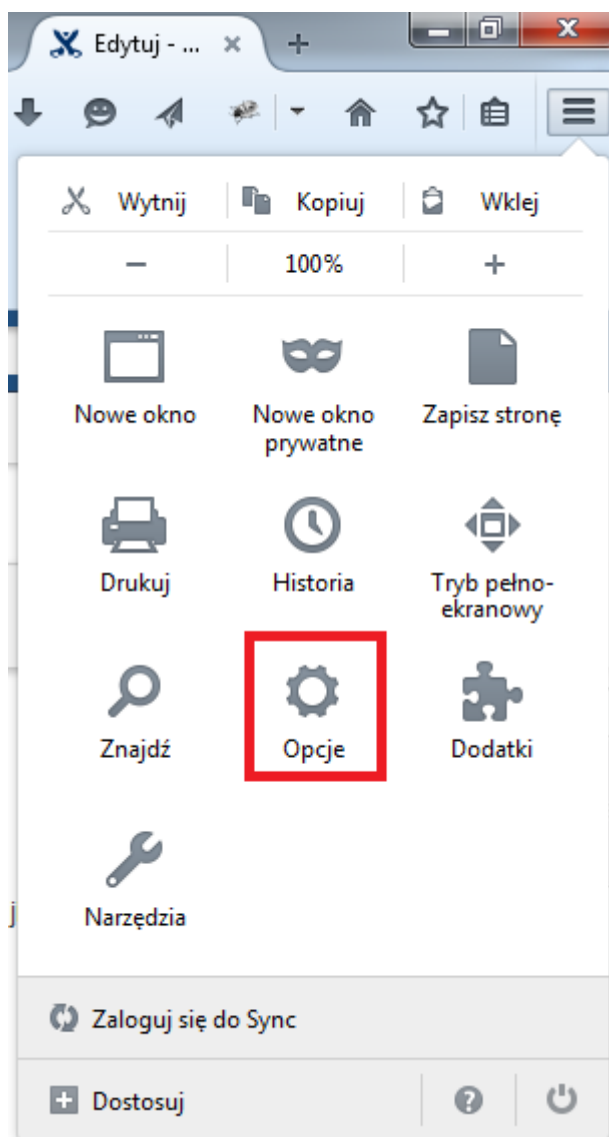
Z uwagi na częste aktualizacje przeglądarki Firefox, które mogą powodować nieprawidłowe działanie systemu SmartCity zalecamy użycie przeglądarki Firefox w wersji 41. Można ją pobrać ze strony:

<https://ftp.mozilla.org/pub/firefox/releases/41.0/win32/pl/> plik o nazwie firefox setup 41.0.exe.

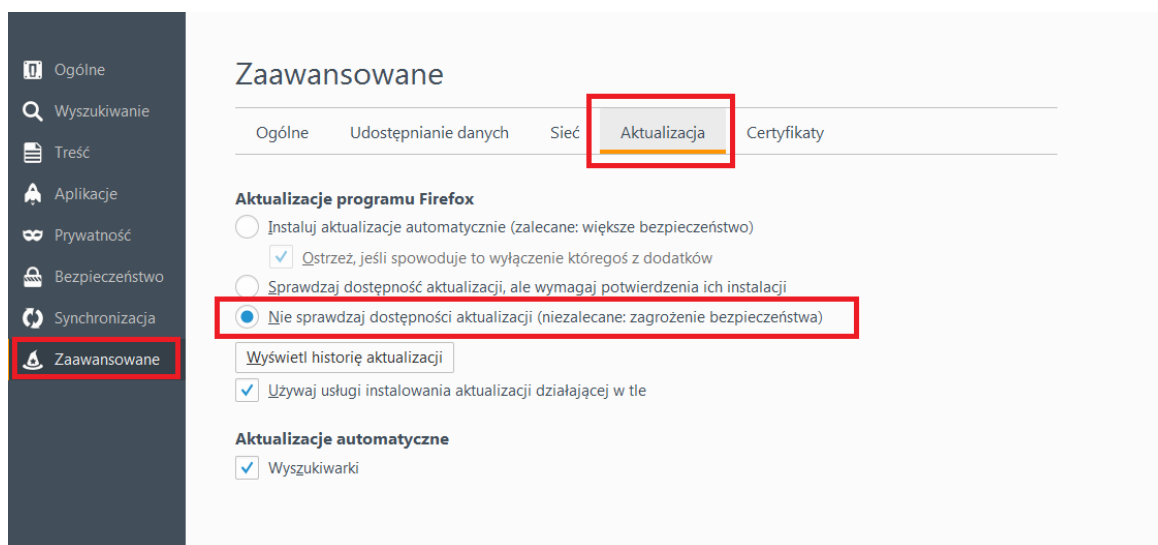
2.3.2.1.2. Wyłączenie aktualizacji

Aby wyłączyć automatyczne aktualizacje, które mogą powodować problemy podczas działania systemu, należy wykonać poniższe kroki:

1. Z menu Firefox wybrać pozycję Opcje



2. Następnie trzeba wybrać menu Zaawansowane, zakładkę Aktualizacja a następnie wybrać opcje *Nie sprawdzaj dostępności aktualizacji*:

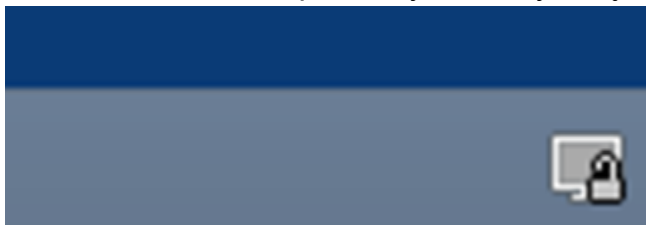


2.3.2.2. Instalacja i konfiguracja OpenVPN

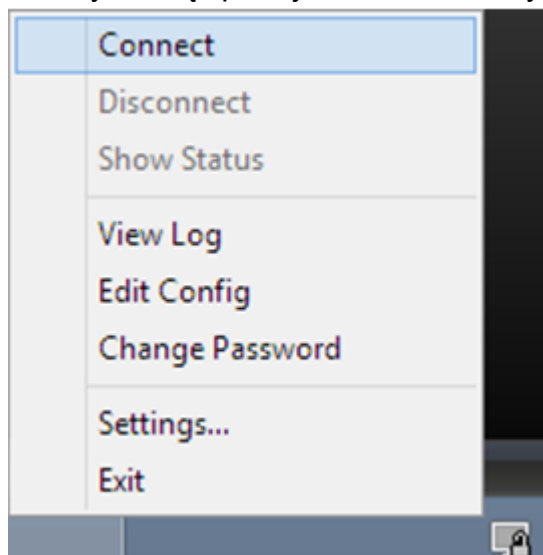
1. Pobrać i zainstalować klienta OpenVPN z: <https://openvpn.net/index.php/open-source/downloads.html>. Proszę wybrać odpowiednią dla systemu paczkę.
2. Do katalogu "C:\Program Files\OpenVPN\config" wgrać otrzymany plik z konfiguracją definicji połączenia mka-nazwa_uzytkownika-config.ovpn
3. Uruchomić klienta OpenVPN poprzez wybranie "**Uruchom jako administrator**" (prawy przycisk) na ikonie



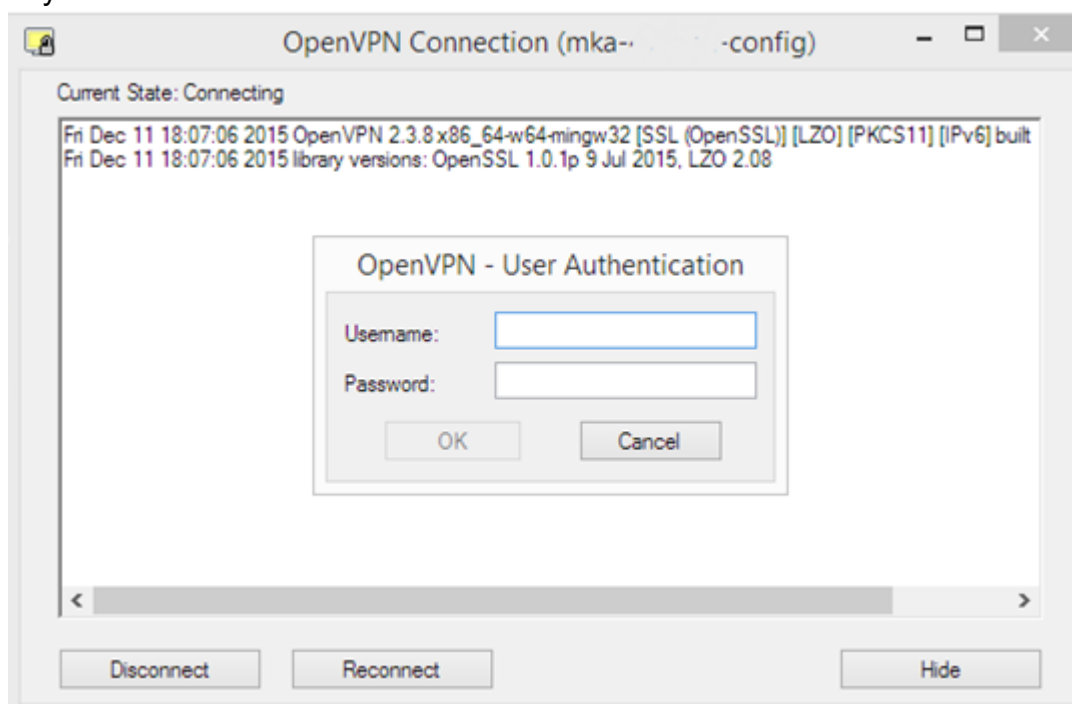
4. Po uruchomieniu na pasku systemowym będzie widoczna ikona



Należy kliknąć prawym klawiszem myszy i wybrać "Connect".



5. Pojawi się okno logowania, proszę wpisać otrzymane dane logowania: użytkownik i hasło.



6. Po nawiązaniu połączenia ikonka na pasku stanu zmieni kolor na zielony.

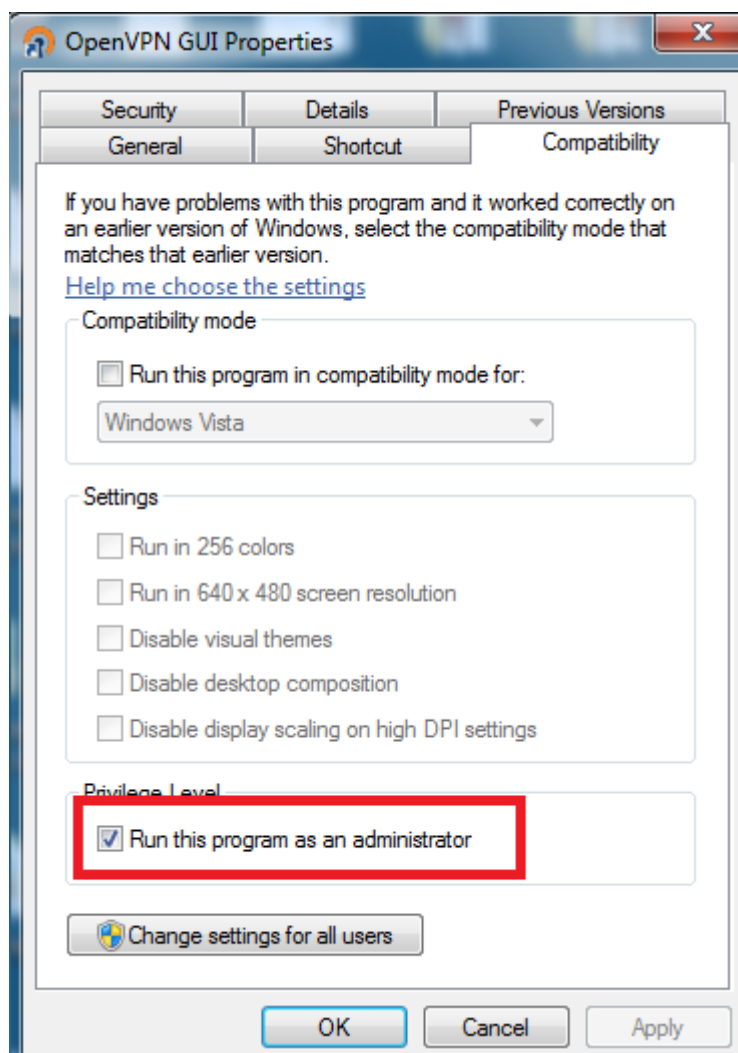


7. Można za pomocą przeglądarki internetowej łączyć się z:
 dane usunięte- system produkcyjny
 dane usunięte - system testowy
8. Po zakończeniu pracy w systemie SmartCity należy wyłączyć tunel poprzez -
 ikona na pasku, prawy klawisz "Disconnect".

Istnieje możliwość ustawienia aby OpenVPN uruchamiał się automatycznie jako administrator (to co zostało wykonane w punkcie 3 powyżej)

Uruchomić właściwości OpenVPN poprzez wybranie "Właściwości"/"Properties" (prawy przycisk) na ikonie OpenVPN znajdującej się na pulpicie.

Przejsć na zakładkę "Compatibility":

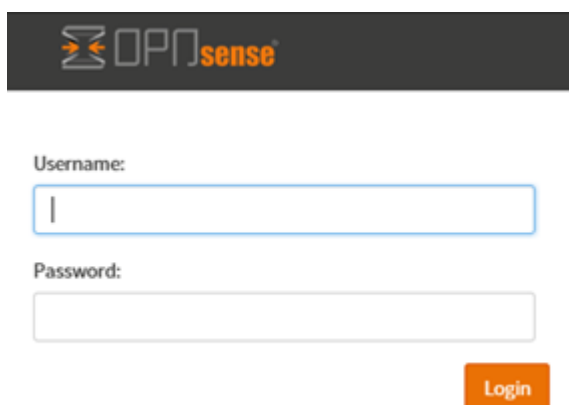


Oznaczyć checkbox przy "Run this program as an administrator".

UWAGA: Po tym uruchomienie OpenVPN będzie mogło odbywać poprzez dwukrotne kliknięcie lewym przyciskiem na ikonę OpenVPN.

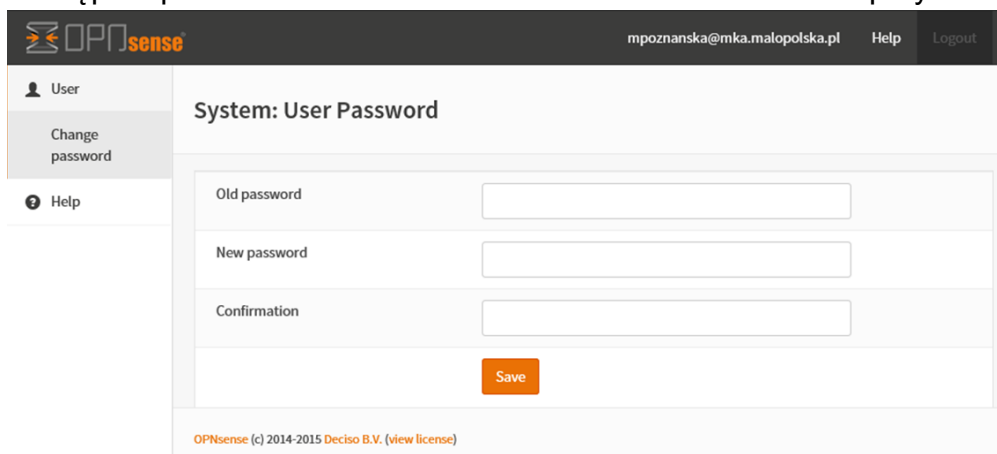
2.3.2.2.1. Zmiana hasła

W celu zmiany hasła do tunelu przy włączonym tunelu należy połączyć się ze stroną dane usunięte i zalogować otrzymanymi danymi logowania: użytkownik i hasło.



The screenshot shows the OPNsense login interface. At the top is the OPNsense logo. Below it are two input fields: 'Username:' and 'Password:'. The 'Username:' field contains a single character 'l'. Below the password field is an orange 'Login' button.

Następnie podać stare hasło i dwukrotnie nowe i zatwierdzić przyciskiem "Save"



The screenshot shows the 'System: User Password' page in OPNsense. The top header includes the OPNsense logo, the email 'mpoznanska@mka.malopolska.pl', and links for 'Help' and 'Logout'. A left sidebar contains 'User', 'Change password', and 'Help'. The main content area has the title 'System: User Password' and three input fields: 'Old password', 'New password', and 'Confirmation'. An orange 'Save' button is at the bottom. A footer note reads: 'OPNsense (c) 2014-2015 Deciso B.V. (view license)'.

Wylogować się poprzez wybranie "Logout" w prawym górnym rogu strony.

2.3.2.3. Java

2.3.2.3.1. Wersja

Do poprawnego działania stacji POK niezbędna jest instalacja środowiska Java. Wersją wymaganą jest wersja nie starsza niż Java 8u60. Aktualną wersję środowiska Java można pobrać ze strony: <https://www.java.com/pl/download/>.

2.3.2.3.2. Wyłączenie automatycznych aktualizacji

Z powodu częstych zmian w Java, które mogą wpływać na jakość działania systemu rekomendujemy wyłączenie automatycznej aktualizacji Javy. W tym celu należy wykonać poniższe kroki:

1. Należy wybrać kolejno Start -> Panel sterowania
2. Uruchomić Java Control Panel
3. Przejść na zakładkę Update

Należy odznaczyć pole Check for Updates Automatically (Automatycznie wyszukuj aktualizacje).

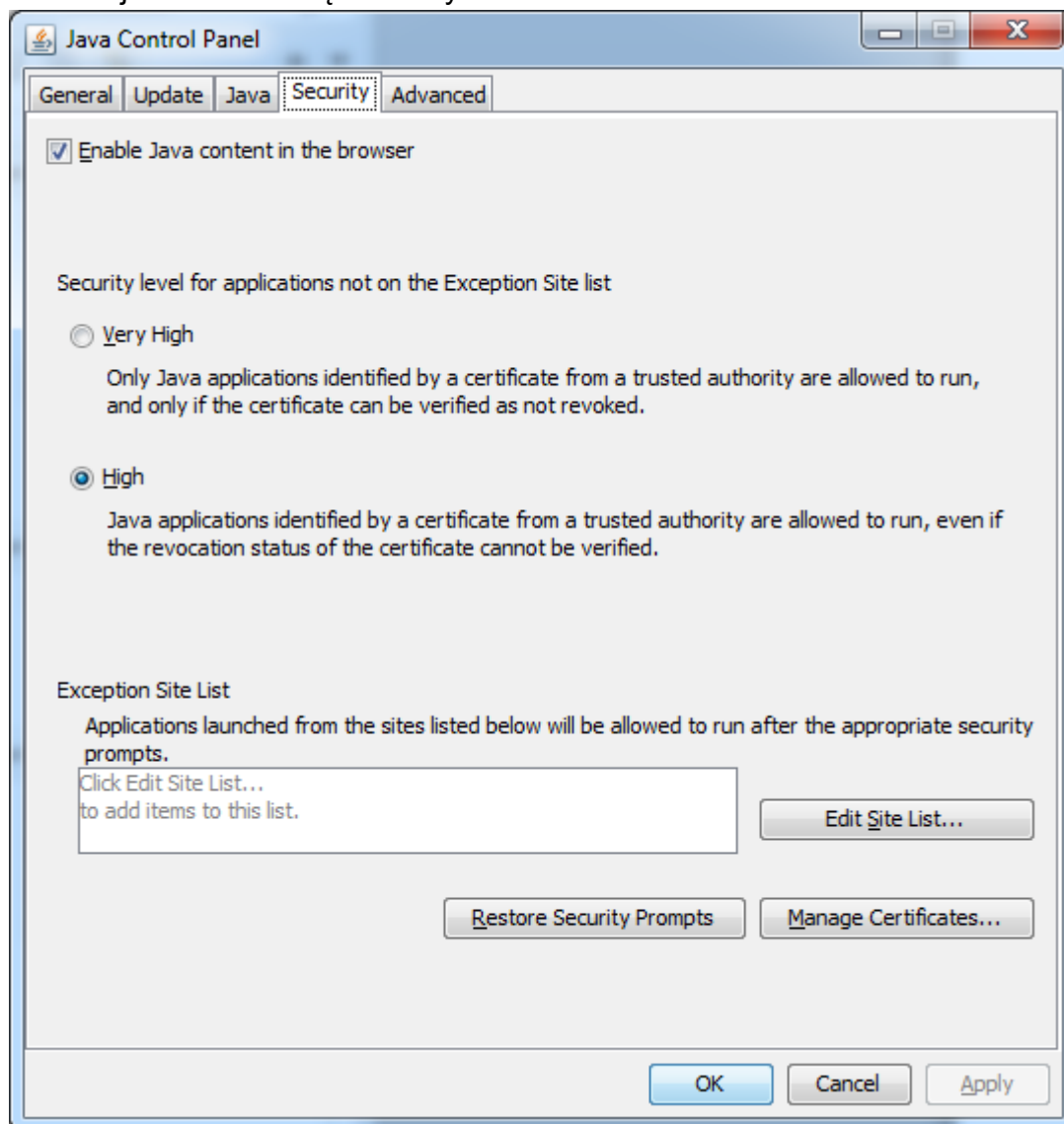
2.3.2.3.3. Ustawienie zabezpieczeń

W sytuacji, gdy podczas uruchamiania SmartCity pojawia się komunikat przedstawiony poniżej, należy wykonać następujące kroki.

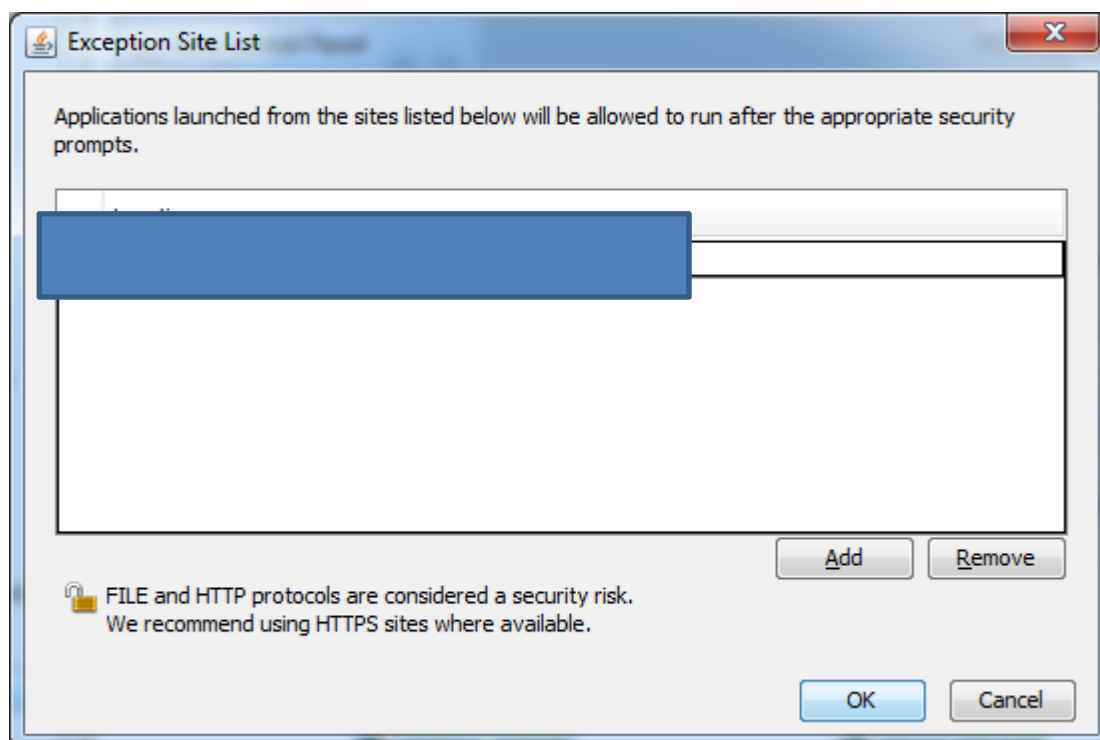


Zamknij okno wybierając OK, a następnie:

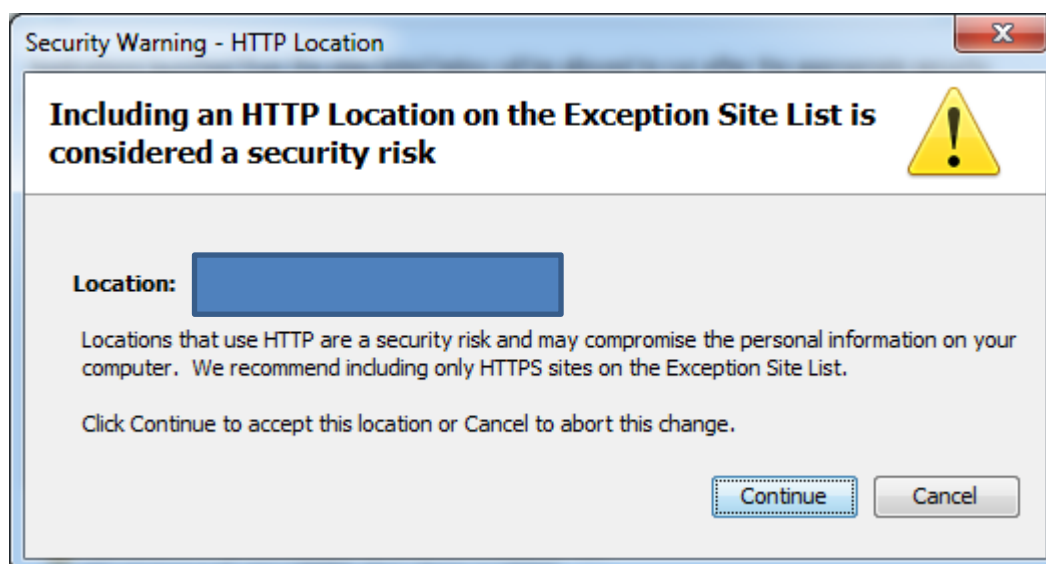
1. Należy wybrać kolejno Start -> Panel sterowania
2. Uruchomić Java Control Panel
3. Przejść na zakładkę Security.



4. W części Exception Site List wybierz przycisk Edit Site List.
5. W pustym wierszu wpisać adres SmartCity MKA w polu Location, tak jak w poniższym oknie:



6. Należy wybrać przycisk Add, a w następnym oknie wybrać przycisk kontynuacji:

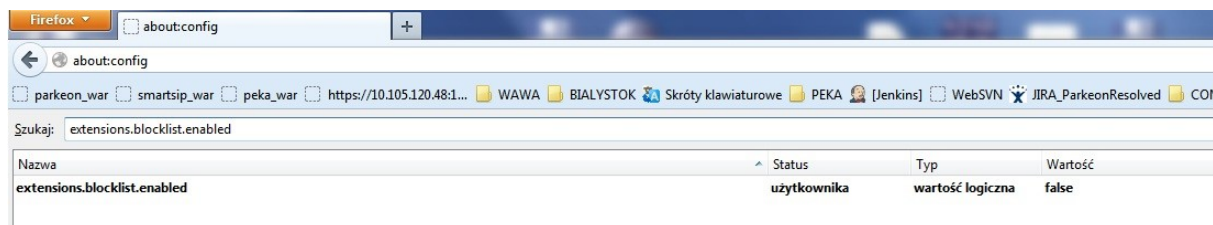


2.3.2.3.4. Wyłączenie automatycznego blokowania Javy

Do prawidłowego działania systemu należy wyłączyć blokowanie Javy. W tym celu należy:

1. W pasku adresu przeglądarki Firefox wpisać about:config

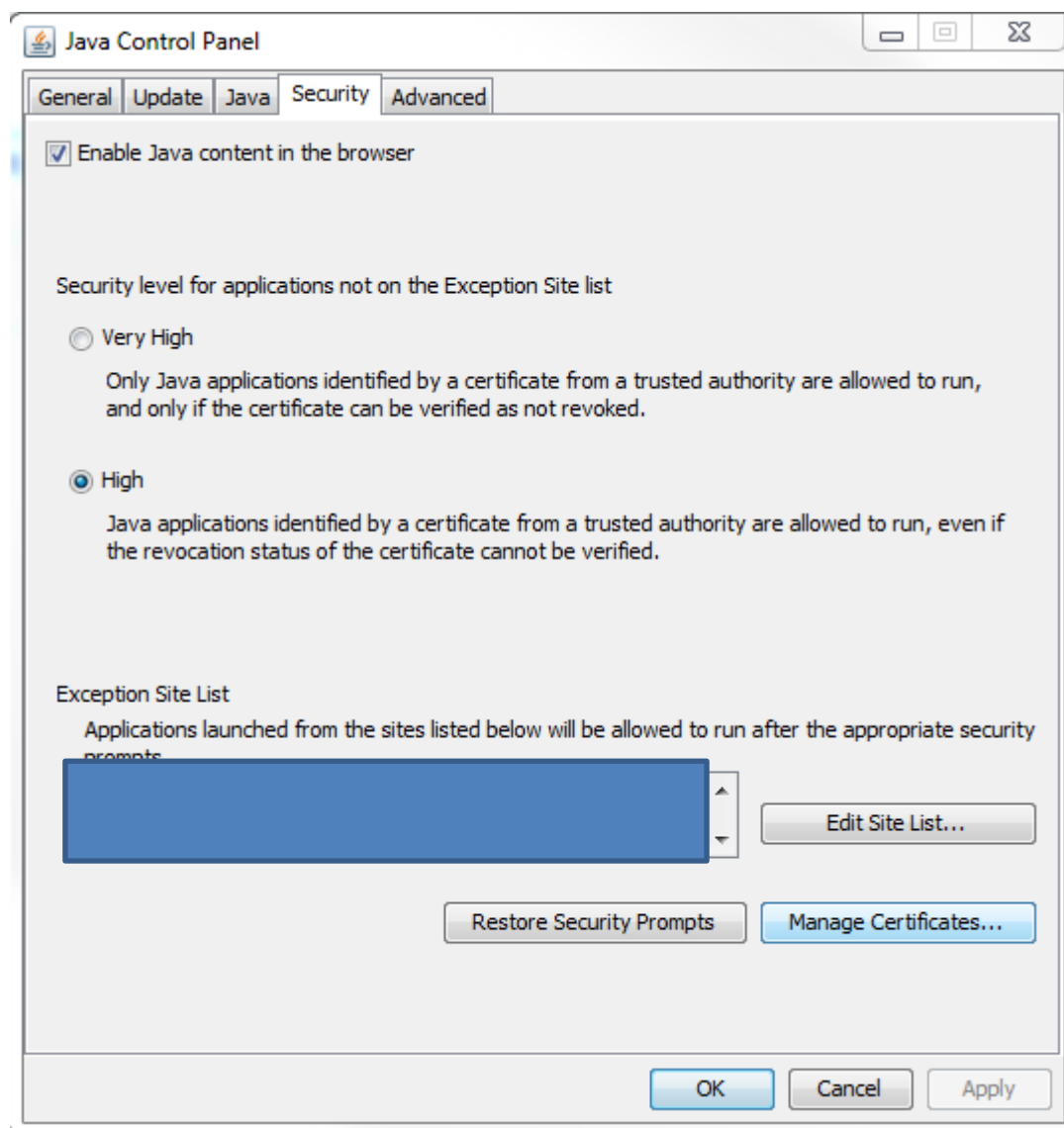
2. W pasku szukaj wpisać: `extensions.blocklist.enabled`
3. Zmienić wartość na false klikając dwa razy na dany wiersz.



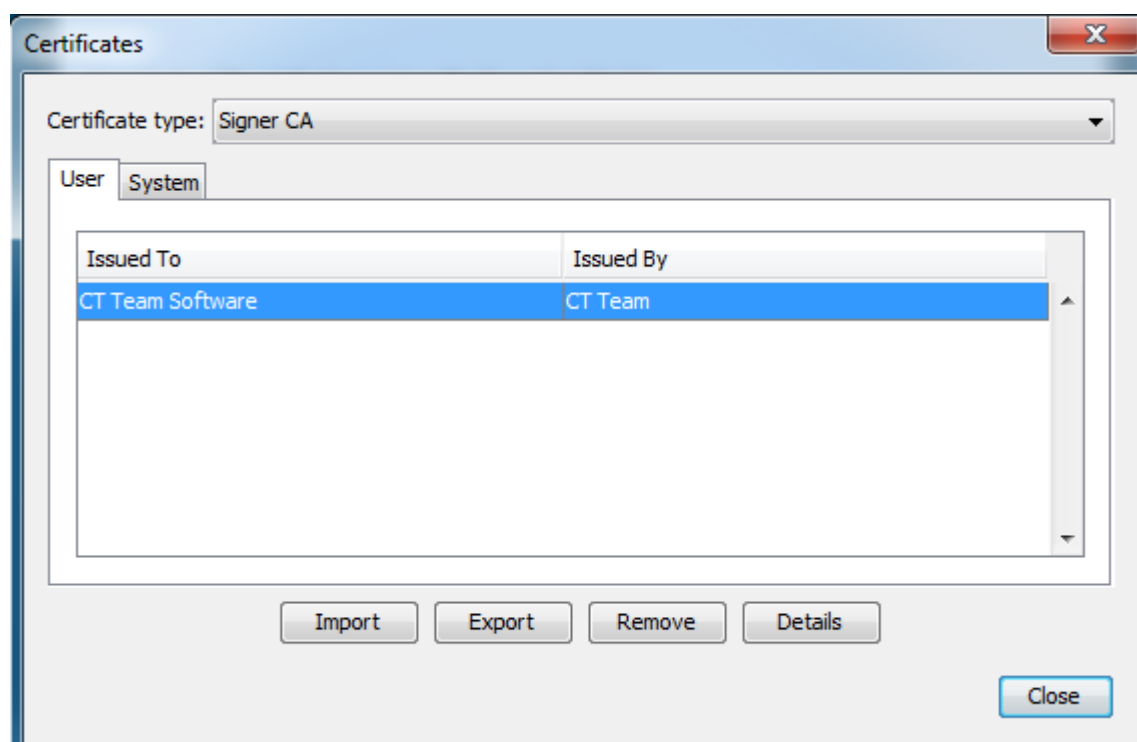
2.3.3. Certyfikat

Aby nie pojawiało się okienko Security Warning dotyczącego appletu to należy zaimportować certyfikat z dołączony do dokumentu. Należy wykonać poniższe kroki:

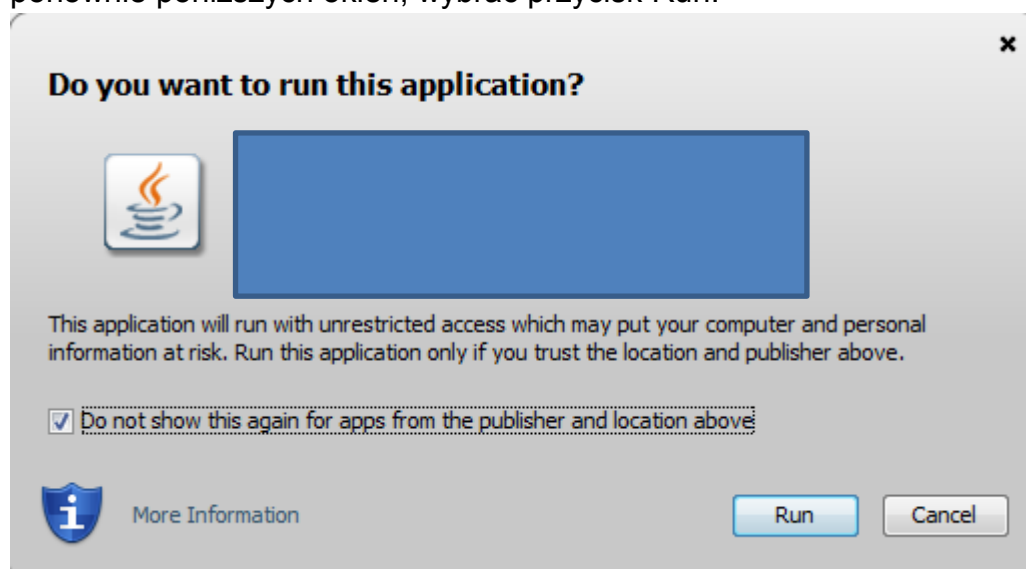
1. Należy wybrać kolejno Start -> Panel sterowania
2. Uruchomić Java Control Panel
3. Przejść na zakładkę Security.
4. Wybrać przycisk Manage Certificates:



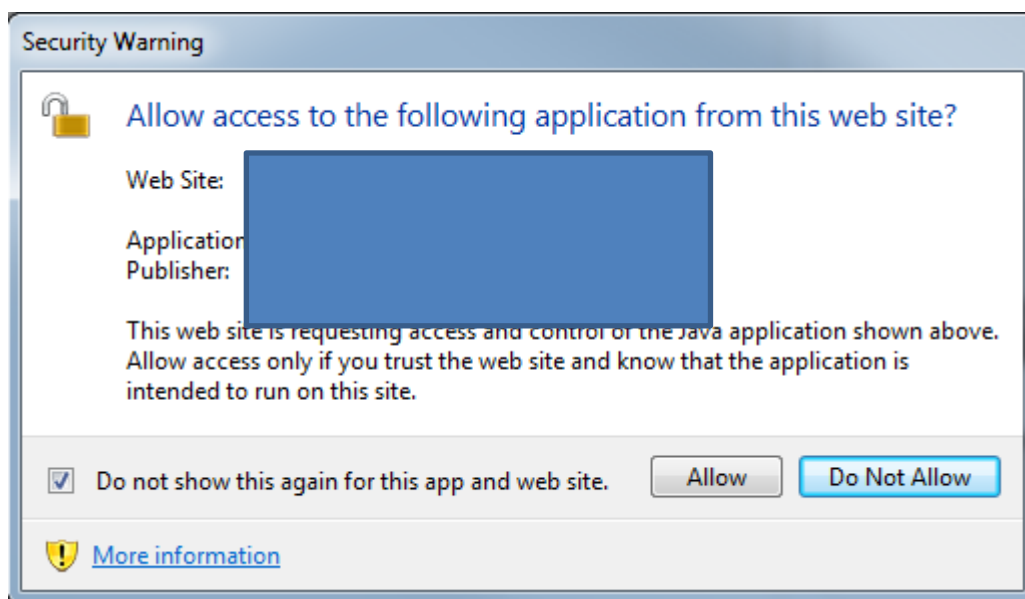
5. Spośród listy Certificate type wybrać Signer CA.
6. Wybrać przycisk Import, odnaleźć plik z certyfikatem na dysku i załączyć:



7. Wybrać przycisk Close, a następnie OK.
8. Uruchomić SmartCity i zaufać dostawcy CT TEAM, zaznaczając niewyświetlanie ponownie poniższych okien, wybrać przycisk Run.



9. Oznaczyć checkbox i wybrać przycisk Allow.



2.3.4. Konfiguracja SmartCity

2.3.4.1. Dodawanie stacji PC

Aby komputer działał prawidłowo musi zostać dodany do systemu SmartCity. W tym celu jako Administrator wchodzimy kolejno w:

1. Zarządzanie Wyposażeniem - > Urządzenia
2. Klikamy przycisk Utwórz
3. Uzupełniamy poszczególne dane, w polu **Ident. fizyczny** wpisując adres MAC komputera

2.3.4.2. Konfiguracja użytkownika

Aby użytkownik mógł korzystać z czytnika kart, a także prawidłowo logować się do Systemu musi zostać odpowiednio skonfigurowany. W tym celu musimy przeprowadzić następujące kroki:

1. Z menu wybieramy Administracja, a następnie zakładka użytkownicy.
2. Wybieramy istniejącego użytkownika, lub klikamy przycisk Utwórz.
3. W nowym oknie uzupełniamy niezbędne dane (razem z dowiązaniem do roli oraz z prawem dostępu do danych)
4. Jeśli uzupełniliśmy wszystkie dane wybieramy przycisk Zapisz.

3. Procedury awaryjne

Historia zmian

Wersja	Data	Opis	Autor	Uwagi
0.1	2015-11-04	Utworzenie	Atos	

3.1. Wstęp

Niniejsza dokumentacja stanowi zbiór Procedur awaryjnych. Zawiera informacje przeznaczone dla administratorów, którzy w ramach swoich obowiązków służbowych będą odpowiedzialni za reagowanie w przypadku awarii i usuwanie ich skutków w zakresie systemów i urządzeń stanowiących elementy systemu MKA. Procedury administracyjne obejmują następujące obszary:

- [Procedura przełączenia CPD1=>CPD2](#)
- [Procedura uruchomienia środowiska CPD1 lub CPD2](#)

3.2. Procedura awaryjnego przełączenia systemu MKA do zapasowej serwerowni CPD2.

1. Zalogować się VPN do środowiska produkcyjnego kontem, które umożliwia dostęp do routera znajdującego się pod adresem ip dane usunięte
2. Otworzyć terminal serwera X1.SKA lub innego jeśli ten uległ awarii i uruchomić kod Switch2KRK.sh

Skrypt wykonuje następujące czynności

- a. Wyłącza replikację bazy danych CPD1=>CPD2
- b. Przenosi dostępowe środowiska z sieci 10.0 do 10.1

3. Uruchomić portale na środowisku zapasowe

Serwer	Komenda
Dane usunięte	su - mka portal_start
Dane usunięte	su - mka portal_start

4. Zweryfikować widoczność połączeń:

Serwer	Usługa
http://mka.malopolska.pl	Portal
Dane usunięte	SmarCity

Dane usunięte

3.3. Procedura uruchomienia środowiska CPD1 lub CPD2

Historia zmian

Wersja	Data	Opis	Autor	Uwagi
0.1	2015-11-27	Utworzenie	Atos	

3.3.1. Wstęp

Niniejsza dokument stanowi część dokumentacji Procedur awaryjnych. Dokument zawiera informacje przeznaczone dla administratorów, którzy w ramach swoich obowiązków służbowych będą odpowiedzialni za uruchomienie i utrzymanie środowisk CPD1 i CPD2.

3.3.2. Kroki procedury

Krok 1. Uruchomić Xen Center do ściągnięcia z <http://xenserver.org/open-source-virtualization-download.html>

Krok 2. Podłączyć się do instancji XenServer

XenCenter	Adres
CPD1	Dane usunięte
CPD2 Kraków	Dane usunięte

Krok 3. Włączyć maszyny wirtualne w kolejności z tabelki.

Kluczowe jest uruchomienie i dostępność maszyny DB1 zanim zostaną włączone pozostałe maszyny.

Nr	Maszyna
1	Dane usunięte
2	Dane usunięte
3	Dane usunięte
4	Dane usunięte
5	Dane usunięte
7	Dane usunięte
8	Dane usunięte

Krok 4. Weryfikacja usług

Usługa	Jak sprawdzić w przeglądarce	Oczekiwany rezultat lub działanie sprawdzające
Portal MKA	http://mka.malopolska.pl	Strona główna portalu



SOP	https://mka.malopolska.pl/moje-konto#/login	Brak komunikatu o niedostępności SOP
iMKA	https://mka.malopolska.pl/imka	Komunikat widoczny w przeglądarce: {"result":{"code":2,"debugDescription":"Wystąpił błąd: null","description":"Wystąpił błąd: null"}}
Wirtualny doradca	https://mka.malopolska.pl/wirtualny-doradca	Okienko umożliwiające wpisanie pytania.
SmartCity	Dane usunięte	Strona logowania do smartcity. Należy się zalogować
Integracja	Dane usunięte	Zwrot pliku CSV z czarną listą

Krok 5. Ręczne uruchomienie usług/restart

Serwer/Usługa	Komenda	Lokalizacja logu aplikacji
Serwery dostępowe P1-P6	apachectl restart	/var/log/httpd/*.log
Serwery E oraz S	service wildfly restart	/var/log/wildfly/*.log
Serwery PRT1, PRT2	z użytkownika mka: (su - mka) start_portal start_solr-reader start_solr-writer stop_portal stop_solr-reader stop_solr-writer	/home/mka/logs/
Serwery bazodanowe DB1 i DB2	service postgres-9.4 restart	/var/log/postgresql

Wyłączanie/restart bazy danych

UWAGA: NARUSZENIE KOLEJNOŚCI MOŻE SPOWODOWAĆ BRAK INTEGRALNOŚCI POMIĘDZY DB1 I DB2

Lp.	Serwer	Komenda
1	DB2	service pgpool stop
2.	DB2	service pgpool stop
3.	DB2	service postgresql-9.4 stop

4.	DB1	service postgresql-9.4 stop
----	-----	-----------------------------

Drugim sposobem jest wyłączenie maszyn wirtualnych w kolejności:

1. DB2
2. DB1

4. Procedury backupu

Historia zmian

Wersja	Data	Opis	Autor	Uwagi
0.1	2015-11-04	Utworzenie	Atos	
0.2	2015-12-12	Aktualizacja	Atos	

4.1. Wstęp

Niniejsza dokumentacja stanowi zbiór Procedur backupu. Zawiera informacje przeznaczone dla administratorów, którzy w ramach swoich obowiązków służbowych będą odpowiedzialni za wykonywanie kopii bezpieczeństwa i, w razie konieczności, odzyskiwanie danych z tych kopii w odniesieniu do systemów stanowiących elementy systemu MKA. Procedury administracyjne obejmują następujące obszary:

- [Odtwarzanie danych z kopii bezpieczeństwa](#)
- [Polityka kopii bezpieczeństwa](#)

4.2. Definicje pojęć

Termin/Skrót	Definicja
Kopia zapasowa	Dane, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia.
Polityka kopii zapasowych	Zestaw zasad wykonywania kopii zapasowych
System Kopii Zapasowych	Zestaw narzędzi sprzętowo-programowych umożliwiających zdefiniowanie i wykonywanie kopii zapasowych zgodnie z politykami

4.3. Informacje ogólne o systemie tworzenia kopii bezpieczeństwa

Jako System Kopii Zapasowych użyte zostało urządzenie EMC Avamar znajdujące się w szafie telekomunikacyjnej w serwerowni głównej jako system podstawowy i w serwerowni zapasowej jako kopia. Pomiędzy tymi lokalizacjami jest skonfigurowana replikacja asynchroniczna danych znajdujących się na urządzeniach. EMC Avamar jest podłączony do infrastruktury za pomocą połączeń Ethernet do przełączników HP 3800. Dane zapasowe jak i dane odtworzenia przesyłane będą poprzez sieć LAN.

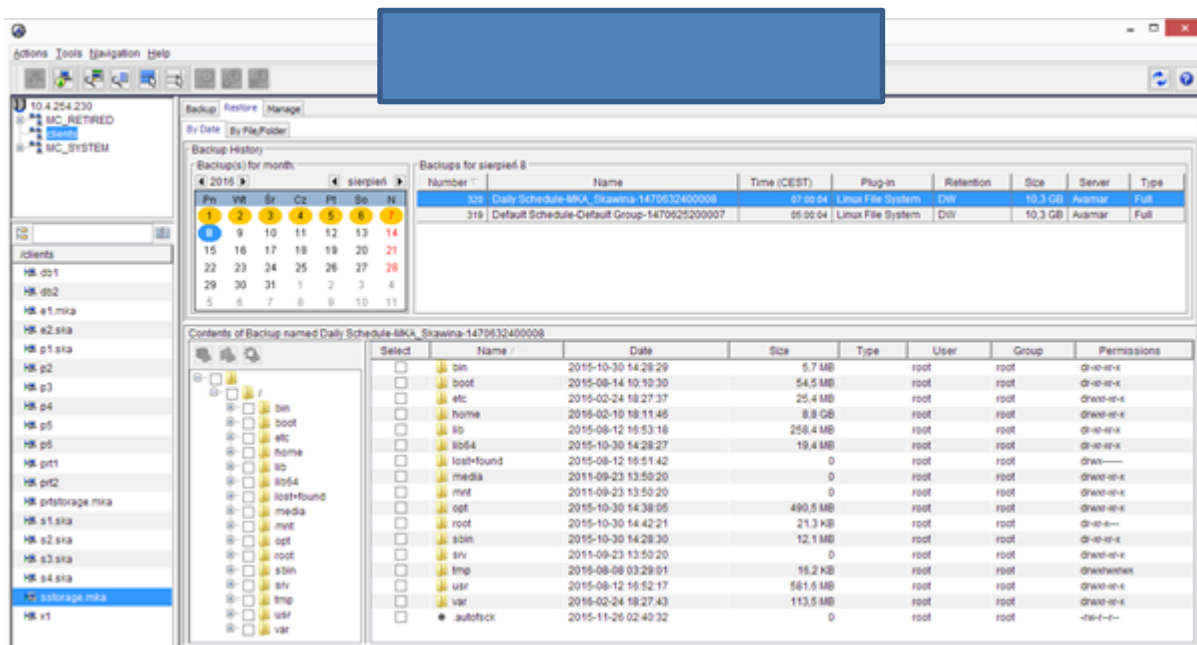
4.4. Odtwarzanie danych z kopii bezpieczeństwa

W celu odtworzenia danych z danego serwera należy:

1. Uruchomić okno administracyjne programu Avamar i wybrać zakładkę "Backup&Restore".
2. Wybrać dany serwer z listy klientów systemu.
3. W oknie "Backup History" wybrać dzień z kalendarza.
4. W oknie "Backups for [wybrana data]" wybrać zestaw kopii

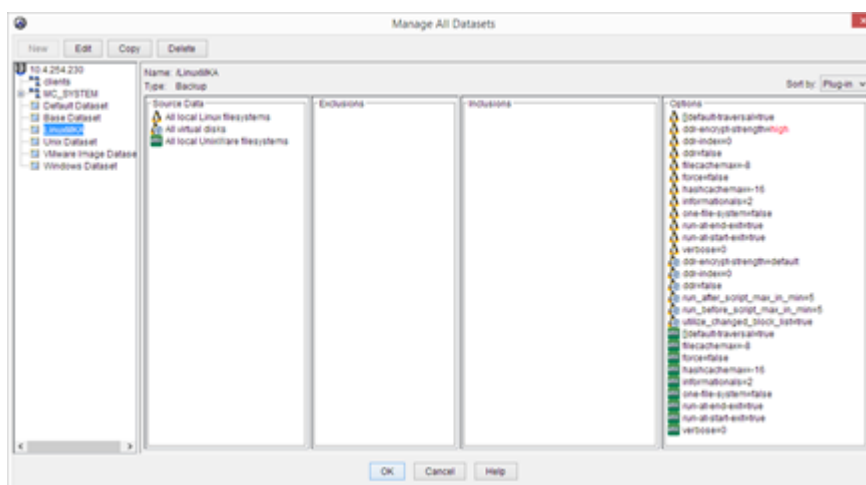
5. W oknie zawartości kopii "Contents of Backup" wybrać w systemie plików interesujący plik, katalog lub ich zestaw.
6. W menu wybrać: "Action-> Restore Now ..."
7. Poprawność wykonania odtwarzania można zweryfikować wybierając w menu: "Action->View Activity". Status operacji powinien wskazywać "Completed".

Widok okna odtwarzania przedstawiony jest na poniższym rysunku:

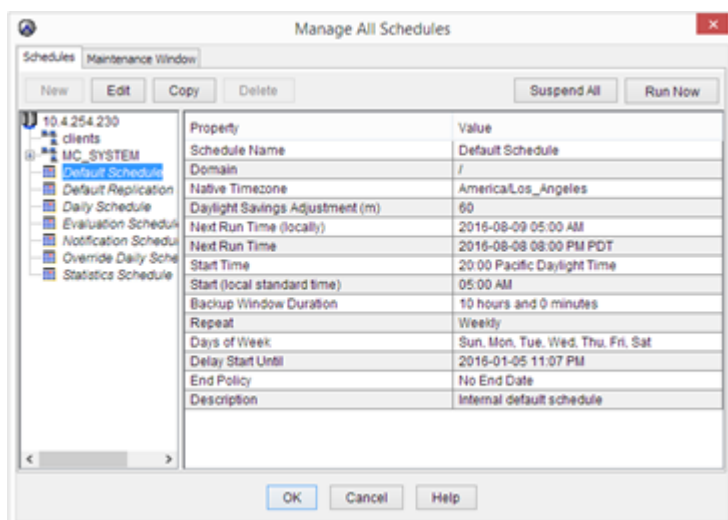


4.5. Polityka kopii bezpieczeństwa

Zestaw danych przeznaczonych do kopiowania jest określony jako "wszystkie lokalne systemy plików" i nazwany "LinuxMKA". Opcje zestawu danych przedstawione są na poniższym rysunku.



Powyższe zakresy danych są kopiowane zgodnie z domyślnym harmonogramem codziennie o godzinie 5:00 bezterminowo. Parametry harmonogramu przedstawione są na poniższym rysunku:



Czas retencji danych jest określony domyślnie na 60 dni.
Lista serwerów podlegających systemowi kopii jest widoczna na poniższym rysunku:



UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO

