OGÓLNOPOLSKA
SIEĆ EDUKACYJNA

Instrukcja wdrożenia usług bezpieczeństwa OSE

przeznaczona dla komputerów z systemem Windows w wersji 7,8,10 w środowisku zarządzanym przez Windows AD

ose.gov.pl

Spis treści

O projekcie Ogólnopolskiej Sieci Edukacyjnej

Ogólnopolska Sieć Edukacyjna (zwana dalej „OSE”) jest projektem konstytuowanym na mocy ustawy z dnia 27 października 2017r. o Ogólnopolskiej Sieci Edukacyjnej (zwanej dalej „Ustawą”).

Zgodnie z Ustawą, OSE jest publiczną siecią telekomunikacyjną, dzięki której szkoły otrzymają nieodpłatny dostęp do szybkiego internetu wraz z usługami bezpieczeństwa sieciowego i teleinformatycznego oraz usługami ułatwiającymi dostęp do technologii cyfrowych.

Operatorem OSE jest Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (zwany dalej „NASK”), nadzorowany przez Ministra Cyfryzacji.

Wstęp

W niniejszej instrukcji opisane zostały czynności wymagane do prawidłowego uruchomienia zamówionych przez szkołę zaawansowanych usług bezpieczeństwa OSE:

- Ochrona przed szkodliwym oprogramowaniem
- Ochrona Użytkownika OSE

Usługi bezpieczeństwa OSE realizowane są na urządzeniach centralnych w sieci OSE. Do ich poprawnego działania wymagana jest inspekcja ruchu szyfrowanego SSL. W tym celu niezbędne jest zainstalowanie certyfikatów SSL, które udostępnia NASK. Zainstaluj je na wszystkich komputerach i urządzeniach przenośnych (laptopy, tablety, smartfony) łączących się z siecią OSE.

W przypadku podłączenia do sieci szkolnej urządzenia nie mającego zainstalowanego certyfikatu SSL (zarówno komputera jak i innych urządzeń przenośnych), usługi bezpieczeństwa nie będą działały prawidłowo, utrudnione będzie korzystanie z internetu na tym urządzeniu, większość stron www będzie wyświetlana nieprawidłowo, lub w ogóle może nie być wyświetlana.

Poprawne wykonanie czynności w niniejszej instrukcji zagwarantuje możliwość prawidłowego korzystania z zasobów internetu w sposób bezpieczny dla użytkowników sieci w szkole. Szczegółowe informacje dotyczące usług bezpieczeństwa w sieci OSE, znajdują się na portalu OSE, pod adresem ose.gov.pl/uslugi-dodatkowe.

Instrukcja instalacji certyfikatów SSL na komputerach w sieci LAN szkoły

Niniejsza instrukcja opisuje sposób instalacji certyfikatów wykonywany na grupie komputerów z systemem Windows w sieci LAN za pomocą Group Policy Object (GPO) Kontrolera Domeny AD.

Certyfikat wraz niniejszą instrukcją dostępny jest na stronie certyfikat.ose.gov.pl. W celu pobrania plików, otwórz przeglądarkę stron www na urządzeniu, na którym zamierzasz zainstalować certyfikat, otwórz powyższą stronę, wyszukaj sekcję poświęconą komputerom z systemem Windows w środowisku Active Directory, a następnie kliknij na Pobierz pliki.

1. Dystrybucja certyfikatów SSL na komputerach klienckich za pomocą Group Policy Object (GPO) Kontrolera Domeny AD.

Poniższa część instrukcji dotyczy sytuacji, gdy w sieci LAN szkoły uruchomiona została Domena Windows wraz z usługą Active Directory (AD), oraz gdy wszystkie komputery w sieci LAN szkoły znajdują się w AD.

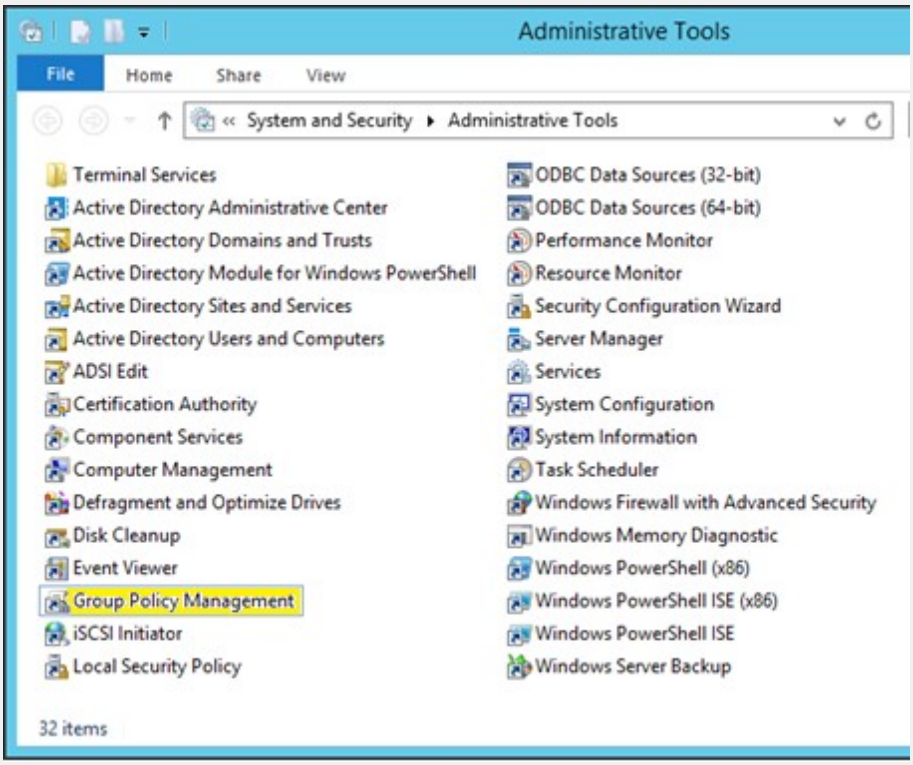
W przypadku gdy w sieci LAN szkoły występują również komputery poza AD, należy do nich zastosować kroki ***Instrukcji instalacji certyfikatów SSL na komputerach z systemem Windows***. Preferowanym rozwiązaniem jest jednak umieszczenie wszystkich komputerów w sieci LAN szkoły w AD.

Do wykonania instrukcji konieczne jest zalogowanie się na Kontrolerze Domeny użytkownika będącego członkiem grupy „Administratorzy domeny” lub równoważnej w AD.

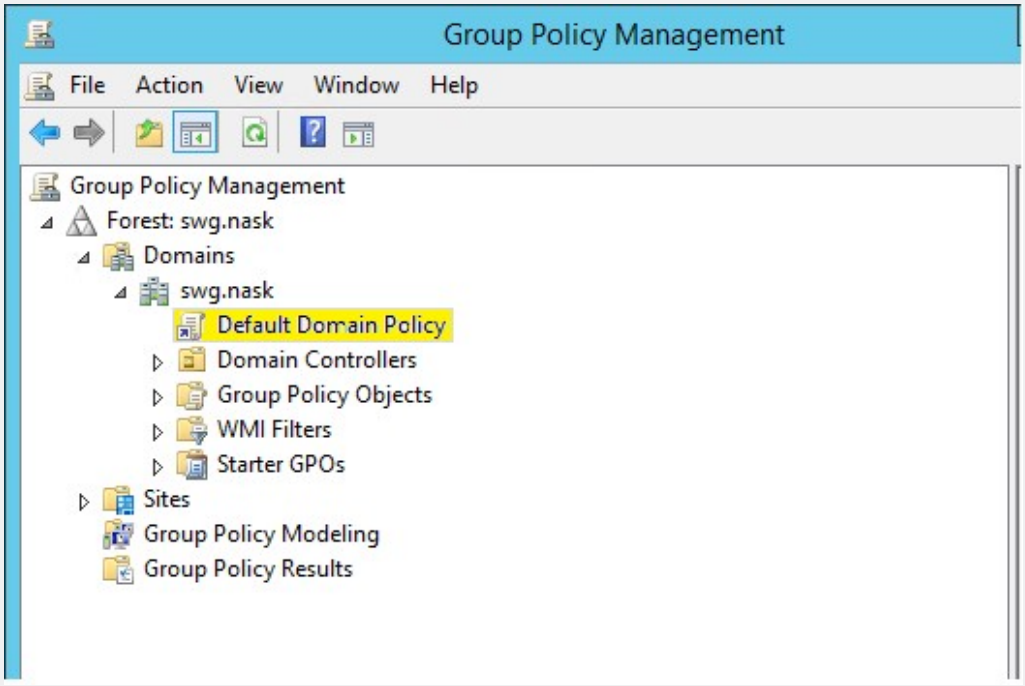
(Poniżej umieszczone zrzuty ekranów zostały wykonane na wersji serwera Windows 2012 R2 w wersji angielskiej).

Aby rozpowszechnić certyfikaty na komputerach klienckich za pomocą AD:

1. Na Kontrolerze Domeny AD otwórz ***Narzędzia Administracyjne (Administrative Tools)*** i kliknij ***Zarządzanie zasadami grupy (Group Policy Management)*.**

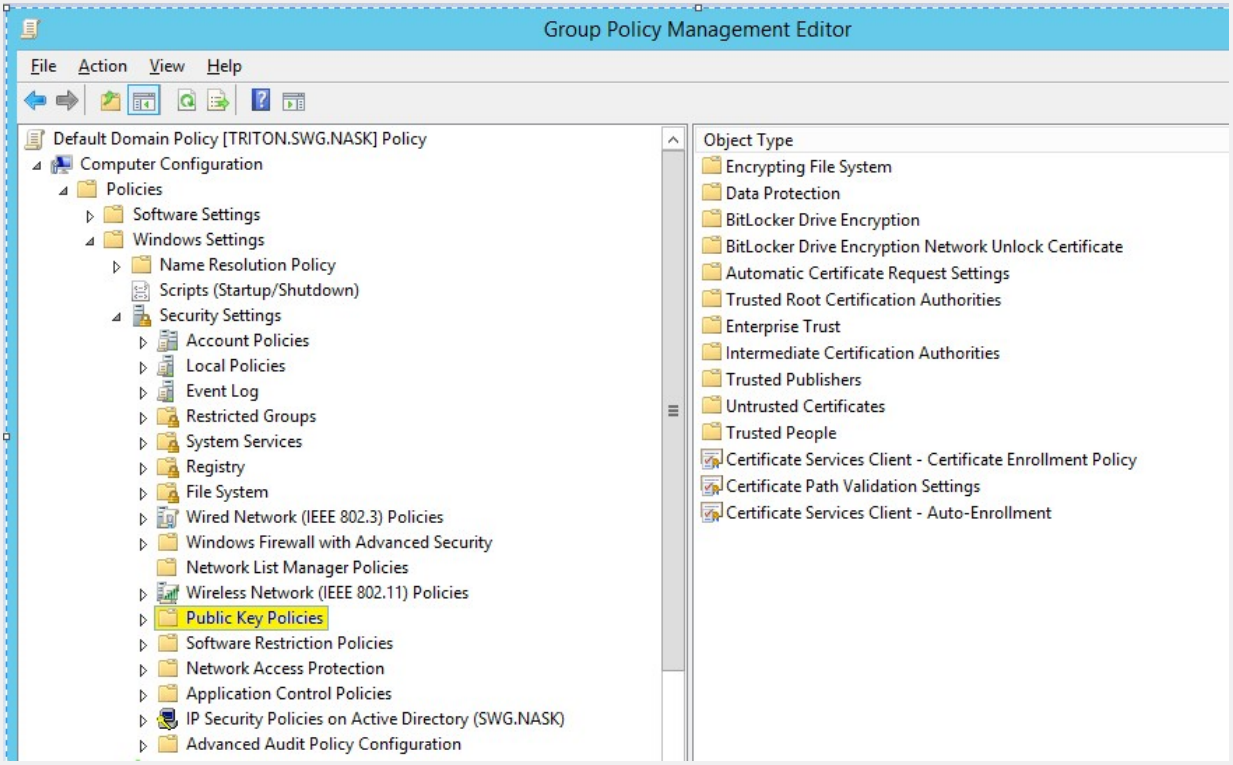


2. Znajdź istniejący domyślny obiekt zasad grupy dla swojej domeny (GPO) lub utwórz nowy obiekt zasad grupy, aby zawierał ustawienia certyfikatu.
   Uwaga: Upewnij się, że obiekt GPO jest skojarzony z domeną, gdzie znajdują się konta użytkowników i komputerów.

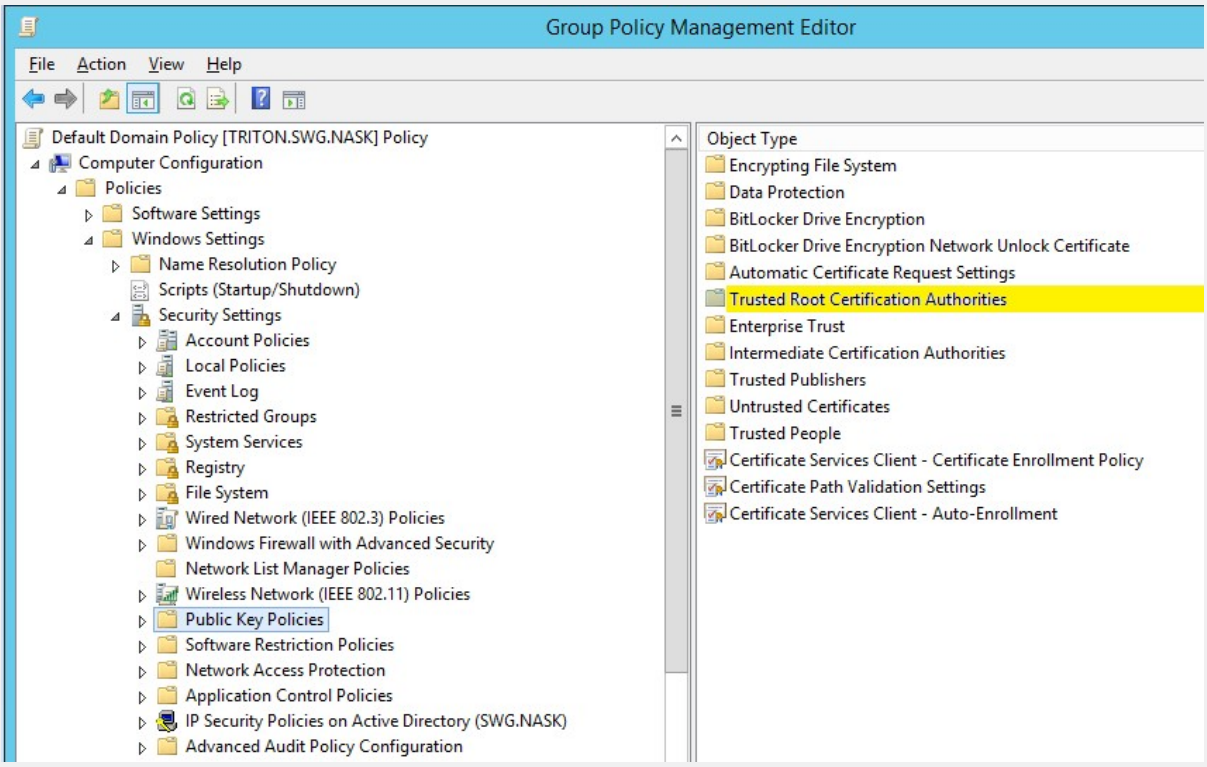


3. Kliknij prawym przyciskiem myszy obiekt zasad grupy, a następnie kliknij polecenie ***Edytuj (Edit)***.

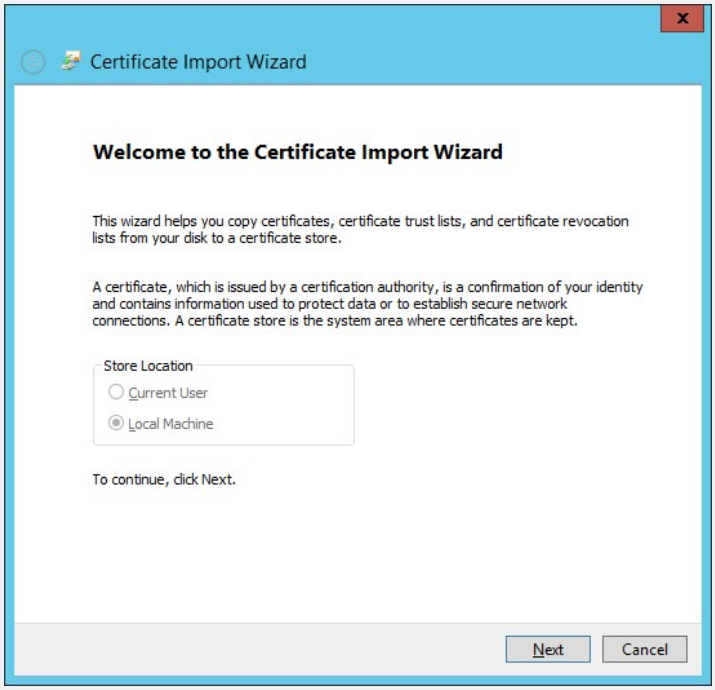
4. W drzewie konsoli otwórz ***Konfiguracja komputera\Zasady\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady kluczy publicznych (Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies)***.



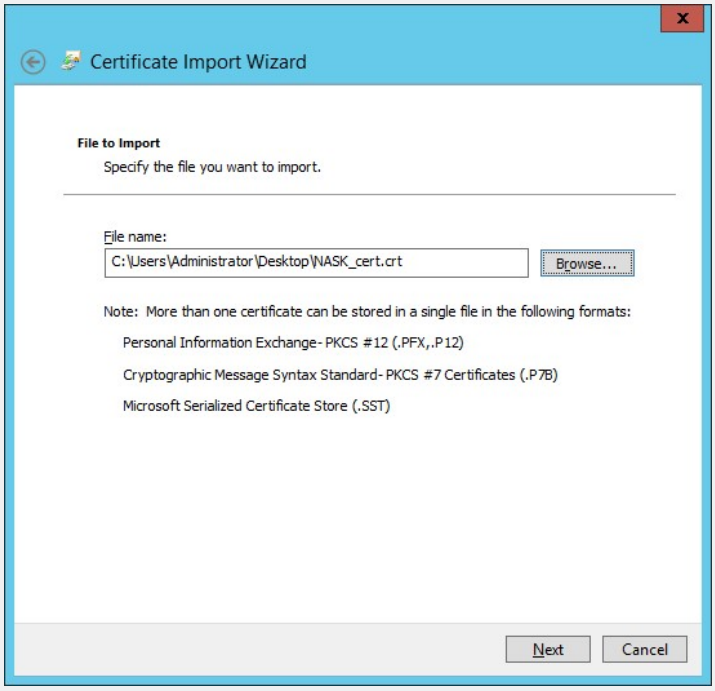
5. Kliknij prawym przyciskiem myszy ***Zaufane główne urzędy certyfikacji (Trusted Root Certification Authorities)***, a następnie kliknij przycisk Importuj.



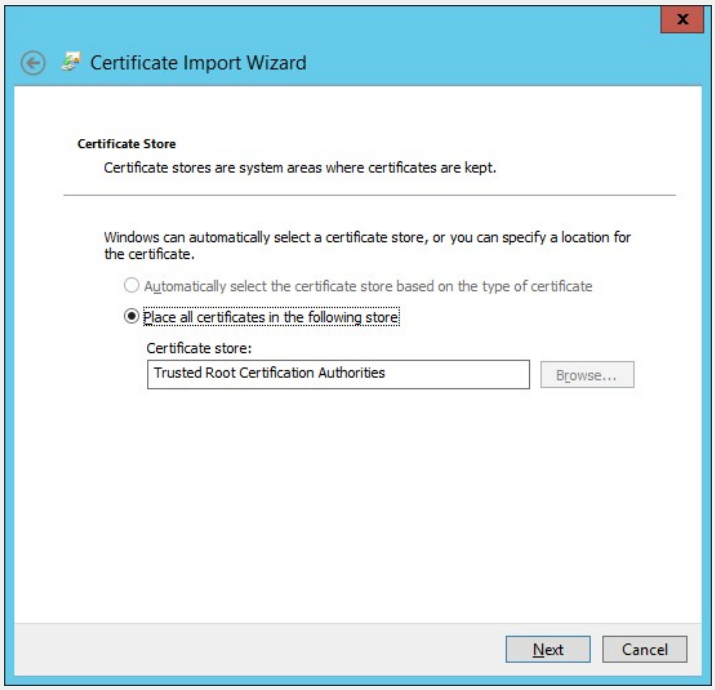
6. W oknie ***Witamy w Kreatorze importu certyfikatów (Welcome to the Certificate Import Wizard)*** kliknij przycisk Dalej (Next).



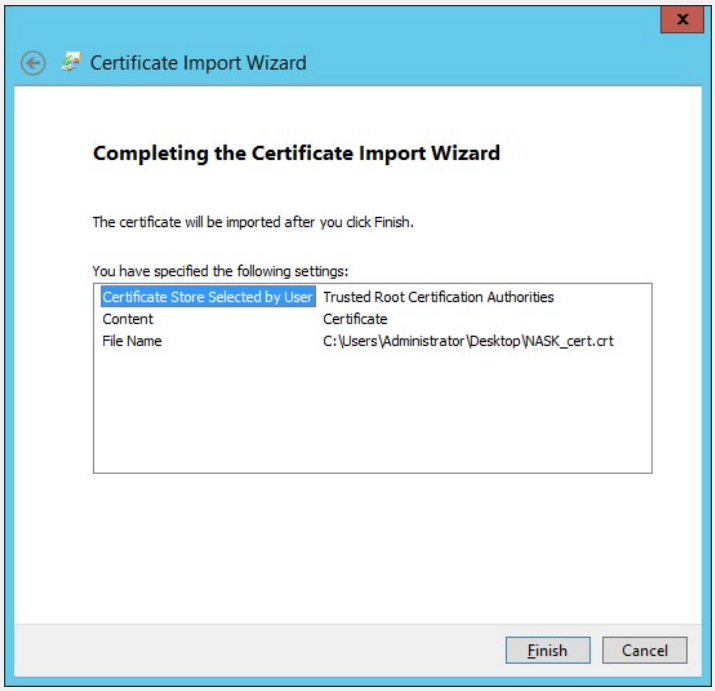
7. W oknie ***Plik do importowania (File to Import)*** wpisz ścieżkę do pliku certyfikatu dostarczonego przez NASK, (np. c:\Users\Administrator\Desktop\certyfikat.crt), a następnie kliknij przycisk ***Dalej (Next)***.



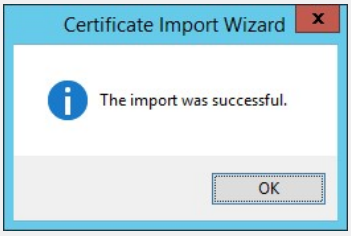
8. W oknie ***Magazyn certyfikatów (Certificate Store)*** kliknij opcję ***Umieść wszystkie certyfikaty w następującym magazynie (Place all certificates in the following store),*** a następnie kliknij przycisk ***Dalej (Next)***.



9. W oknie ***Kończenie pracy Kreatora importu certyfikatów (Completing the Certificate Import Wizard)*** sprawdź, czy podane informacje są dokładne, a następnie kliknij przycisk ***Zakończ (Finish).***



10. Pomyślny import certyfikatu zostanie potwierdzony komunikatem kończącym pracę kreatora.



11. Komputery w sieci LAN szkoły znajdujące się w AD po przelogowaniu się otrzymają zaimportowany certyfikat automatycznie do swoich magazynów systemu Windows.

2. Dystrybucja certyfikatów SSL na komputerach klienckich za pomocą Group Policy Object (GPO) Kontrolera Domeny AD dla przeglądarki Mozilla Firefox.

W przypadku korzystania z zasobów sieci internet za pomocą przeglądarki Mozilla Firefox konieczne jest dodanie certyfikatu SSL dostarczonego przez NASK do systemowego magazynu certyfikatów przeglądarki, ponieważ nie korzysta ona domyślnie z systemowego magazynu certyfikatów systemu Windows.

Poniższa część instrukcji umożliwia dystrybucję za pomocą GPO odpowiednich plików konfiguracyjnych, które zmienią domyślne zachowanie przeglądarki Firefox, na takie które umożliwi korzystanie przez program z systemowego magazynu certyfikatów systemu Windows. Kroki opisane w tej części instrukcji można zastosować tylko w przypadku, gdy w sieci LAN szkoły uruchomiona została Domena Windows wraz z usługą Active Directory (AD), oraz gdy wszystkie komputery w sieci LAN szkoły znajdują się w AD.

W przypadku gdy w sieci LAN szkoły występują również komputery poza AD, należy do nich zastosować kroki ***Instrukcji instalacji certyfikatów SSL na komputerach z systemem Windows***. Preferowanym rozwiązaniem jest jednak umieszczenie wszystkich komputerów w sieci LAN szkoły w AD.

Do wykonania instrukcji konieczne jest zalogowanie się na Kontrolerze Domeny użytkownika będącego członkiem grupy „Administratorzy domeny” lub równoważnej w AD.

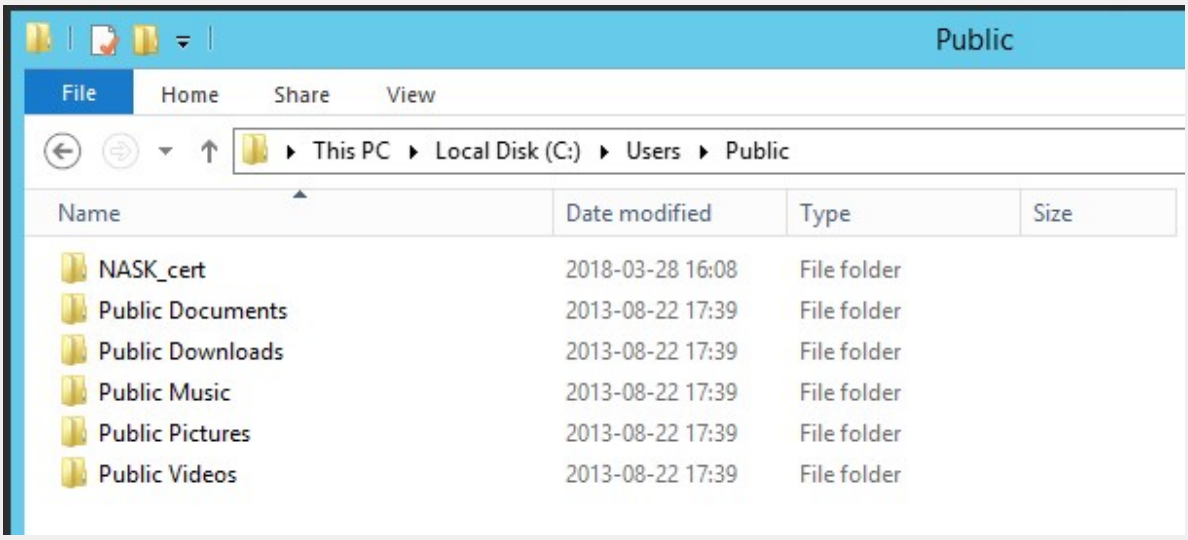
(Poniżej umieszczone zrzuty ekranów zostały wykonane na wersji serwera Windows 2012 R2 w wersji angielskiej).

Aby zmienić domyślną konfigurację przeglądarek Mozilla Firefox na komputerach klienckich za pomocą AD:

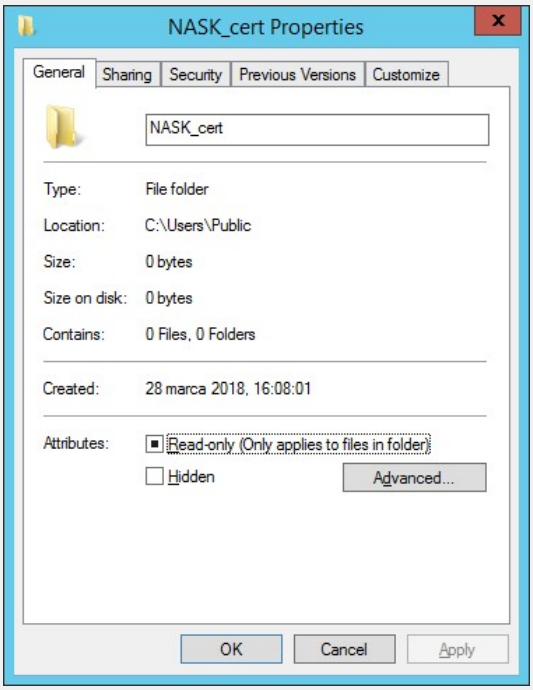
1. Za pomocą edytora tekstu (np. Notepad) utwórz plik ***enableroot.js*** zawierający poniższe polecenie:

   \/ Allows Firefox reading Windows certificates *\/*
   pref("security.enterprise_roots.enabled", true);

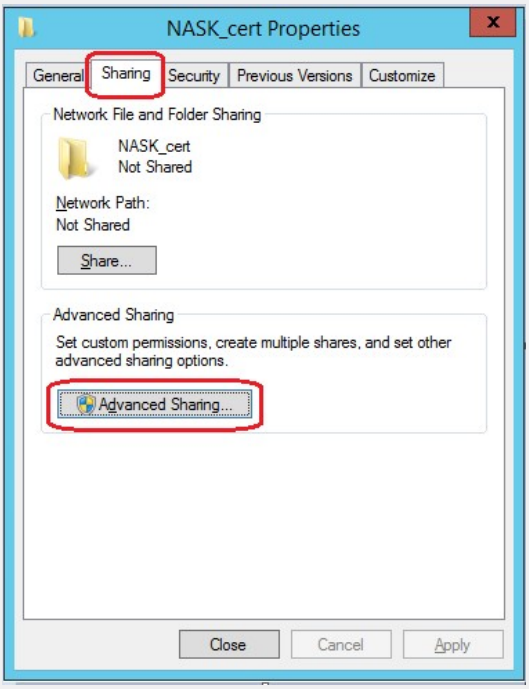
2. Na Kontrolerze Domeny AD utwórz katalog, np.: ***C:\Users\Public\NASK_cert,*** w którym umieść stworzony plik ***enableroot.js***



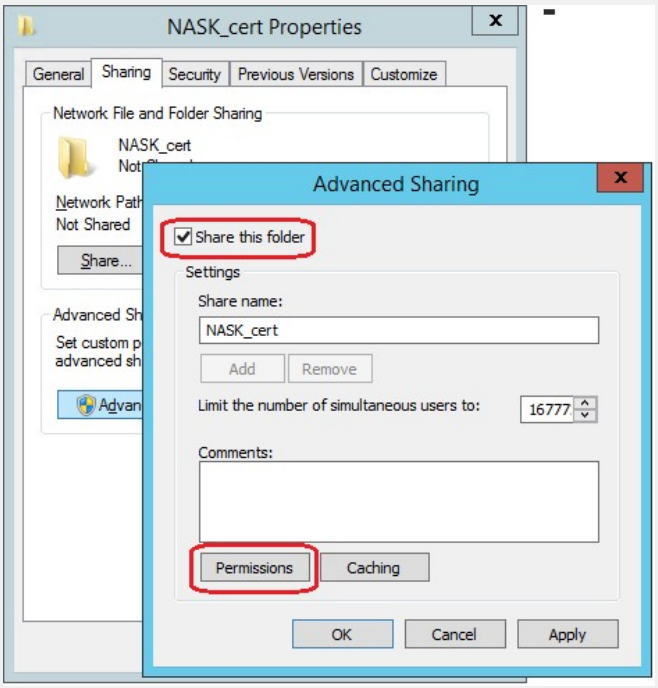
3. Jeśli nadrzędny katalog ***Public*** jest już udostępniony w Domenie Windows, nie musisz robić nic więcej. Jeśli nie jest, udostępnij założony katalog ***NASK_cert*** nadając uprawnienia do jego czytania dla wszystkich użytkowników Domeny Windows. W tym celu:
    a. Kliknij prawym przyciskiem myszy na właśnie stworzonym katalogu i wybierz ***Właściwości (Properties)***



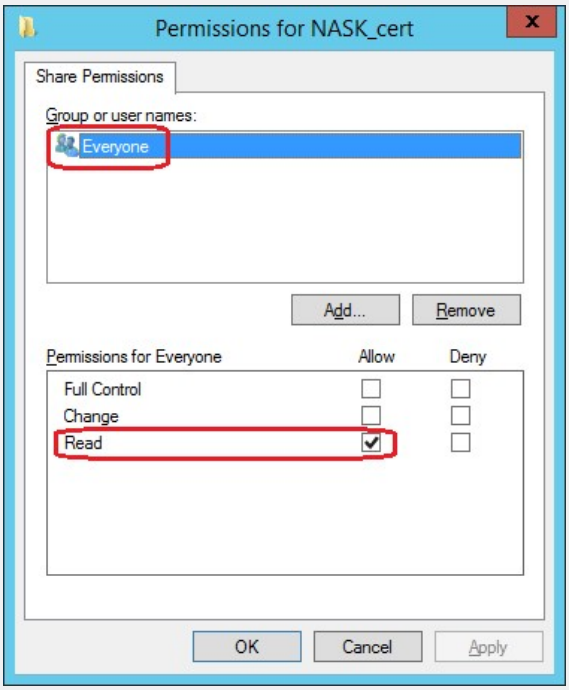
    b. Wybierz zakładkę ***Udostępnianie (Sharing)***, i kliknij przycisk ***Zaawansowane Udostępnianie (Advanced Sharing)***



c. W oknie ***Zaawansowane Udostępnianie (Advanced Sharing)*** zaznacz checkbox ***Udostępnij ten katalog (Share this folder)*** i kliknij przycisk ***Uprawnienia (Permissions)***

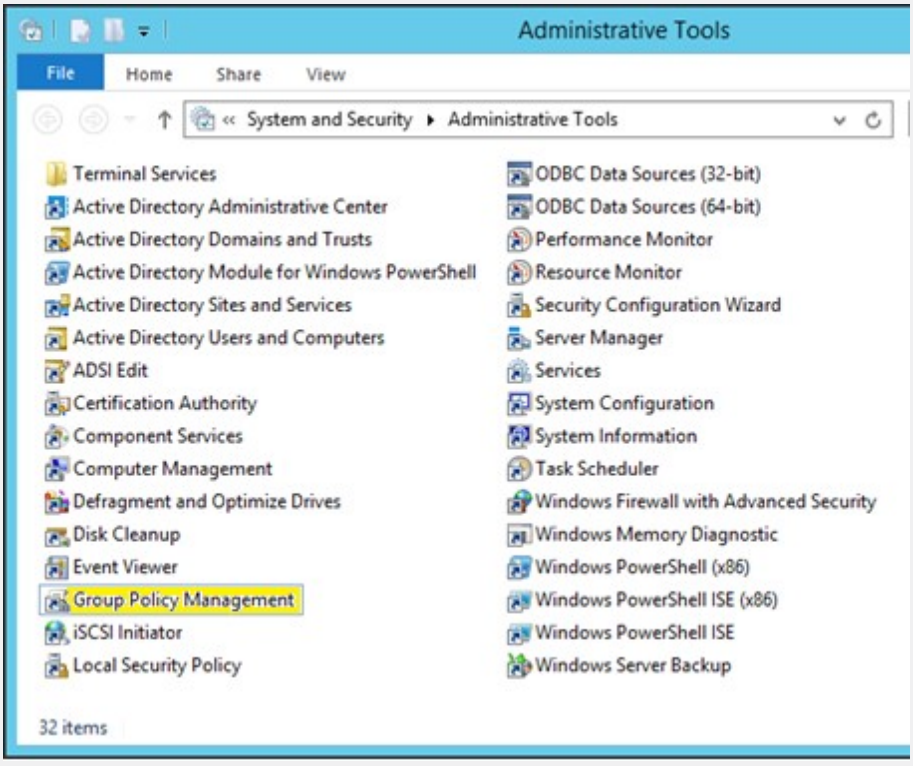


d. W oknie ***Uprawnienia (Permissions for)***dla NASK_cert zaznacz ***Uprawnienia dla Wszyscy do Odczytu (Permissions for Everyone for Read)***



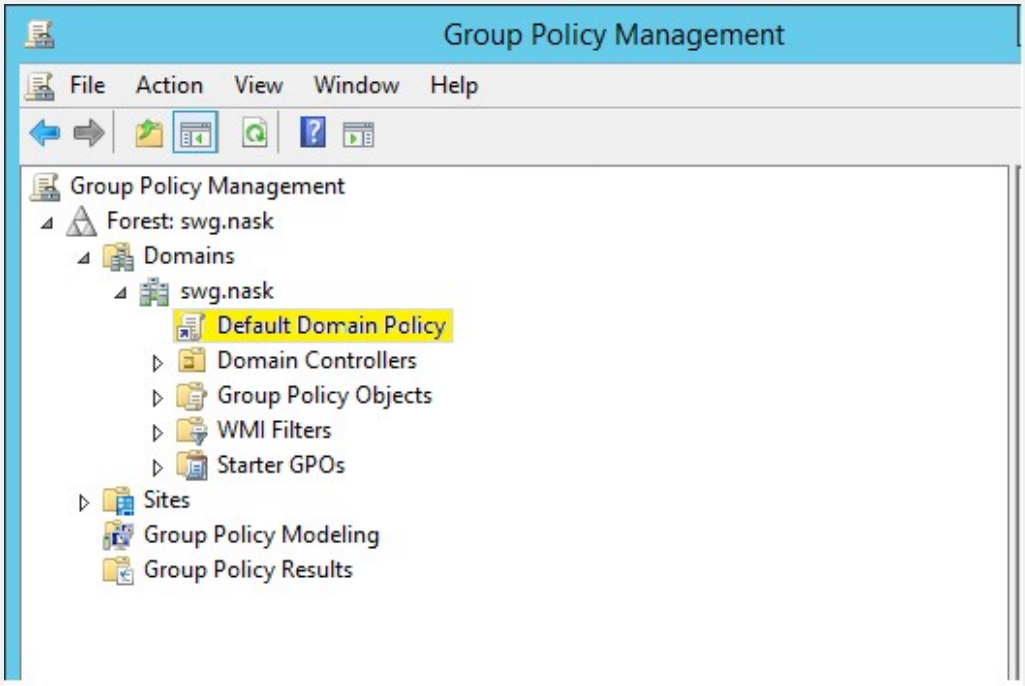
e. Zamknij wszystkie okna klikając kolejno: OK, OK, Zamknij (Close).
f. Poprawność wykonania czynności można zweryfikować wpisując w oknie Eksploratora Windows adres: \\nazwa_serwera\Users\Public\NASK_cert, powinien otworzyć się stworzony przed chwilą katalog.

4. Na Kontrolerze Domeny AD otwórz ***Narzędzia Administracyjne (Administrative Tools)*** i kliknij ***Zarządzanie zasadami grupy (Group Policy Management)*.**



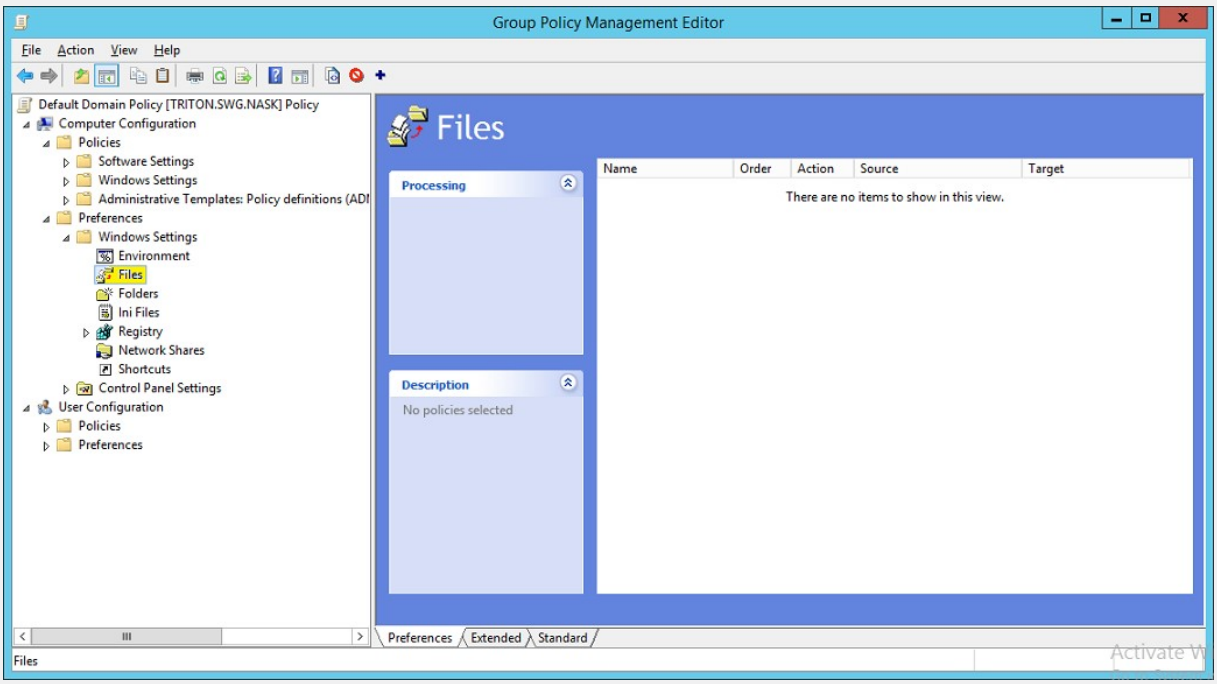
5. Znajdź istniejący domyślny obiekt zasad grupy dla swojej domeny (GPO) lub utwórz nowy obiekt zasad grupy, aby zawierał ustawienia dla przeglądarki Mozilla Firefox.

Uwaga: Upewnij się, że obiekt GPO jest skojarzony z domeną, gdzie znajdują się konta użytkowników i komputerów.

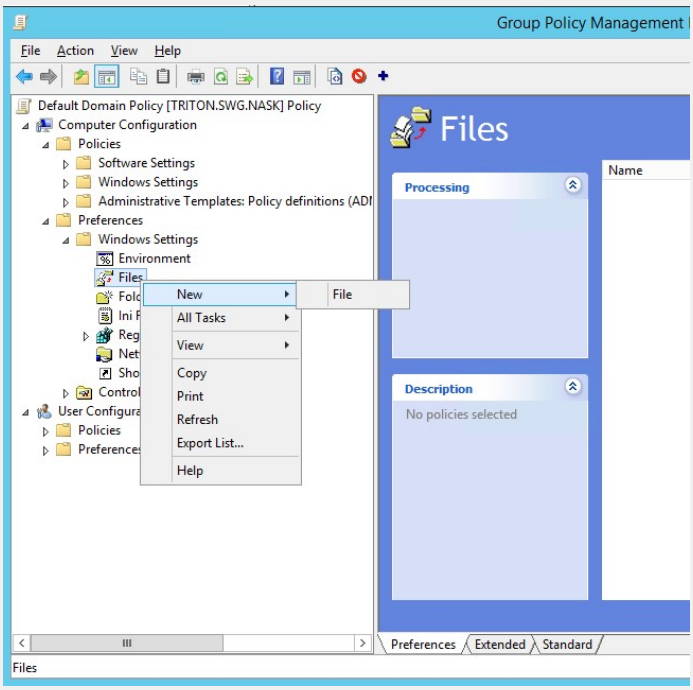


6. Kliknij prawym przyciskiem obiekt zasad grupy, a następnie kliknij polecenie ***Edytuj (Edit)***.

7. W drzewie konsoli otwórz ***Konfiguracja komputera\Preferencje\Ustawienia systemu Windows\Pliki (Computer Configuration\Preferences\Windows Settings\Files)***.



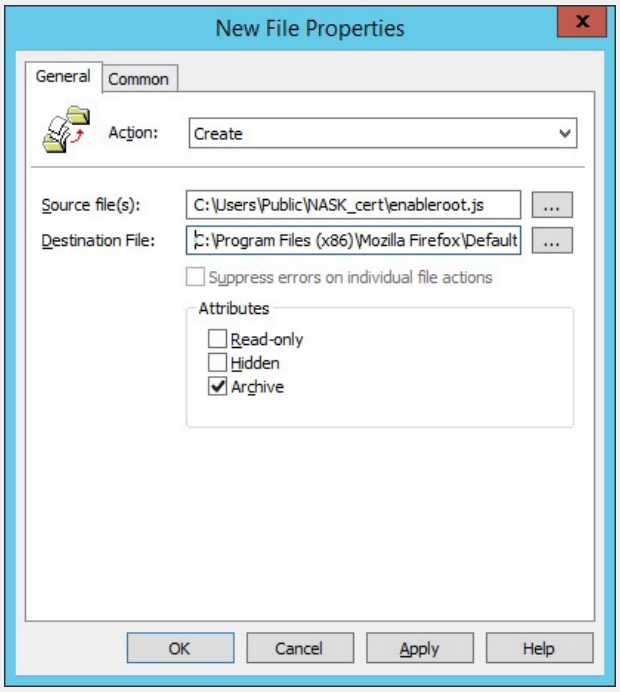
8. Kliknij prawym przyciskiem myszy ***Pliki (Files)*** i wybierz ***Nowy->Plik (New->File)***



9. W Oknie ***Właściwości Nowego Pliku (New File Properties)*** zmień ***Akcję (Action)*** na ***Utwórz (Create)***, W polu ***Pliki źródłowe (Source files)*** wybierz ścieżkę do wcześniej założonego pliku enableroot.js (w naszym przykładzie

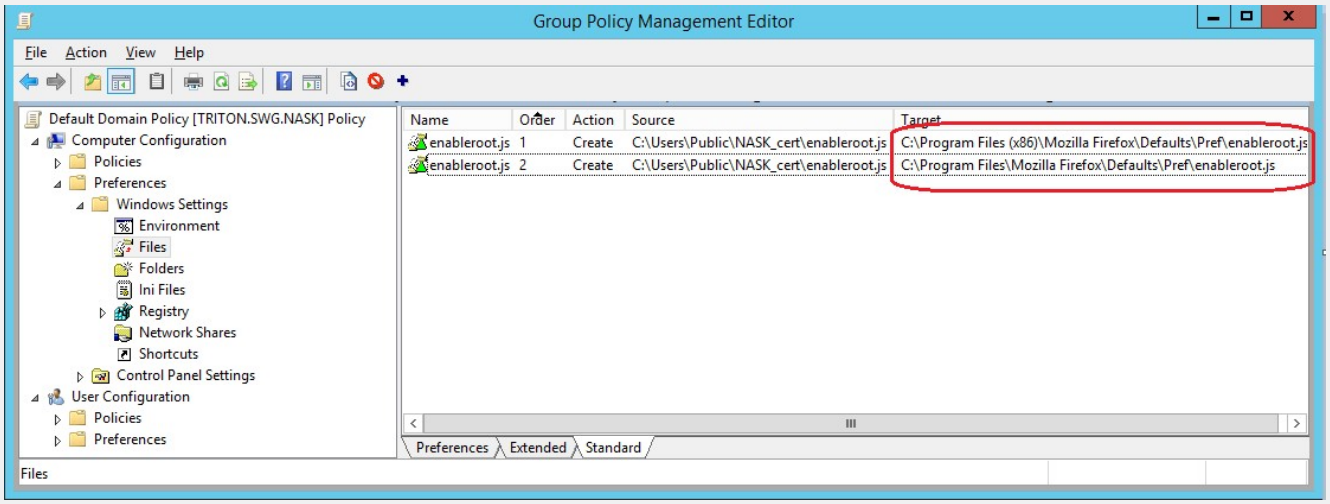
   C:\Users\Public\NASK_cert\enableroot.js). W polu ***Plik Docelowy (Destination File)*** *wpisz*

   C:\Program Files (x86)\Mozilla Firefox\Defaults\Pref\enableroot.js – dla wersji Firefox 64Bit
   C:\Program Files\Mozilla Firefox\Defaults\Pref\enableroot.js - dla wersji Firefox 32Bit



10. Kliknij OK.
11. W przypadku gdy w sieci LAN szkoły znajdują się komputery z zainstalowanymi przeglądarkami w obu wersjach (32bit i 64bit), należy wykonać kopię wpisu (lub

powtórzyć punkty 8-10) i zmienić polecenie w polu ***Plik Docelowy (Destination File),*** tak aby dostępne były konfiguracje dla obu wersji przeglądarek.



12. Komputery w sieci LAN szkoły z zainstalowanymi przeglądarkami Mozilla Firefox otrzymają pliki konfiguracyjne po przelogowaniu się.

T +48 22 182 55 55
ose@ nask.pl

A ul. Kolska 12
01-045 Warszawa

W ose.gov.pl

NIP 5210417157
REGON 010464542

Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
OSE Ogólnopolska Sieć Edukacyjna
Unia Europejska Europejski Fundusz Rozwoju Regionalnego
Ministerstwo Cyfryzacji
NASK