

Zadania do samodzielnej realizacji w domu (Moduł 3)

Zadanie 1

Jesteś administratorem systemów w firmie X.

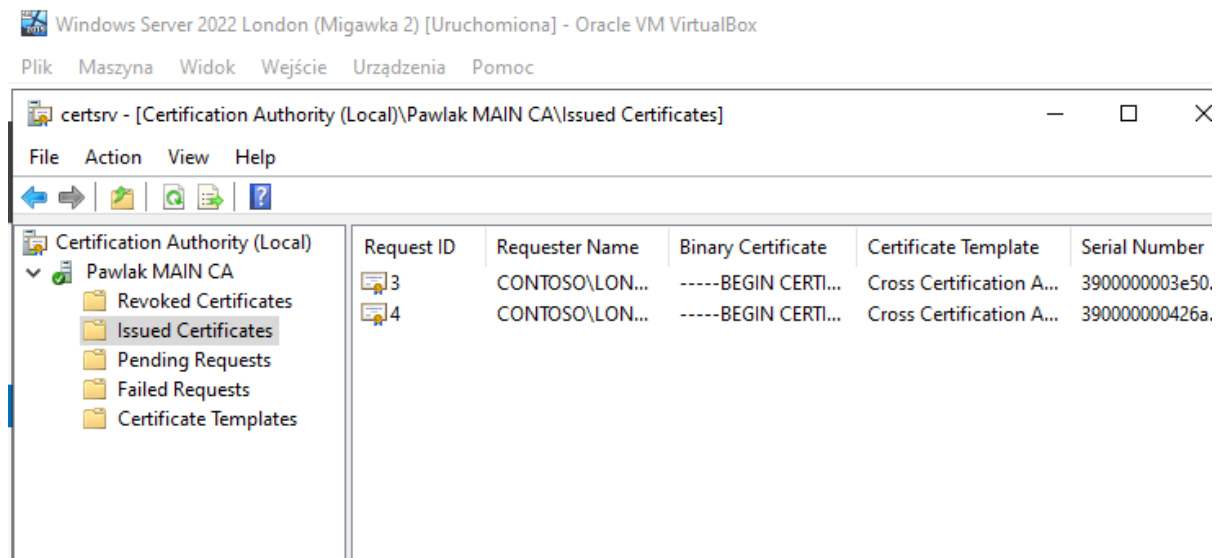
W organizacji zapadła decyzja, aby wdrożyć lokalną infrastrukturę klucza publicznego zintegrowaną z usługą Active Directory, na kontrolerze domeny Windows Server "London".

Twoim zadaniem jest więc zainstalowanie głównego serwera certyfikującego zintegrowanego z usługą Active Directory w systemie Windows Server "London", dla którego należy określić nazwę "{Nazwisko} MAIN CA" (gdzie pod {Nazwisko} należy podstawić własne nazwisko - jest to warunkiem zaliczenia sprawozdania, przykładowo: Kowalski MAIN CA), instalując rolę "Usługi certyfikatów Active Directory" wraz z usługami roli: "Urząd certyfikacji" oraz "Rejestracja w sieci Web dla urzędu certyfikacji".

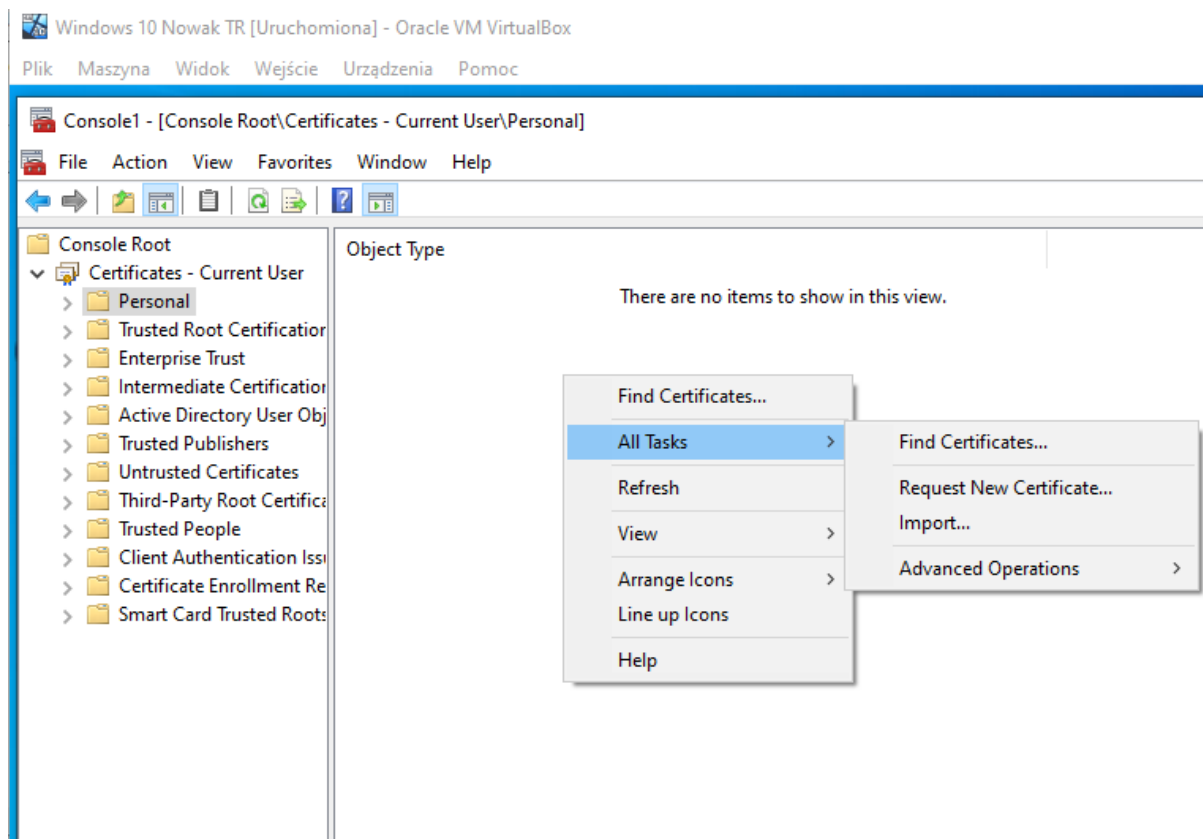
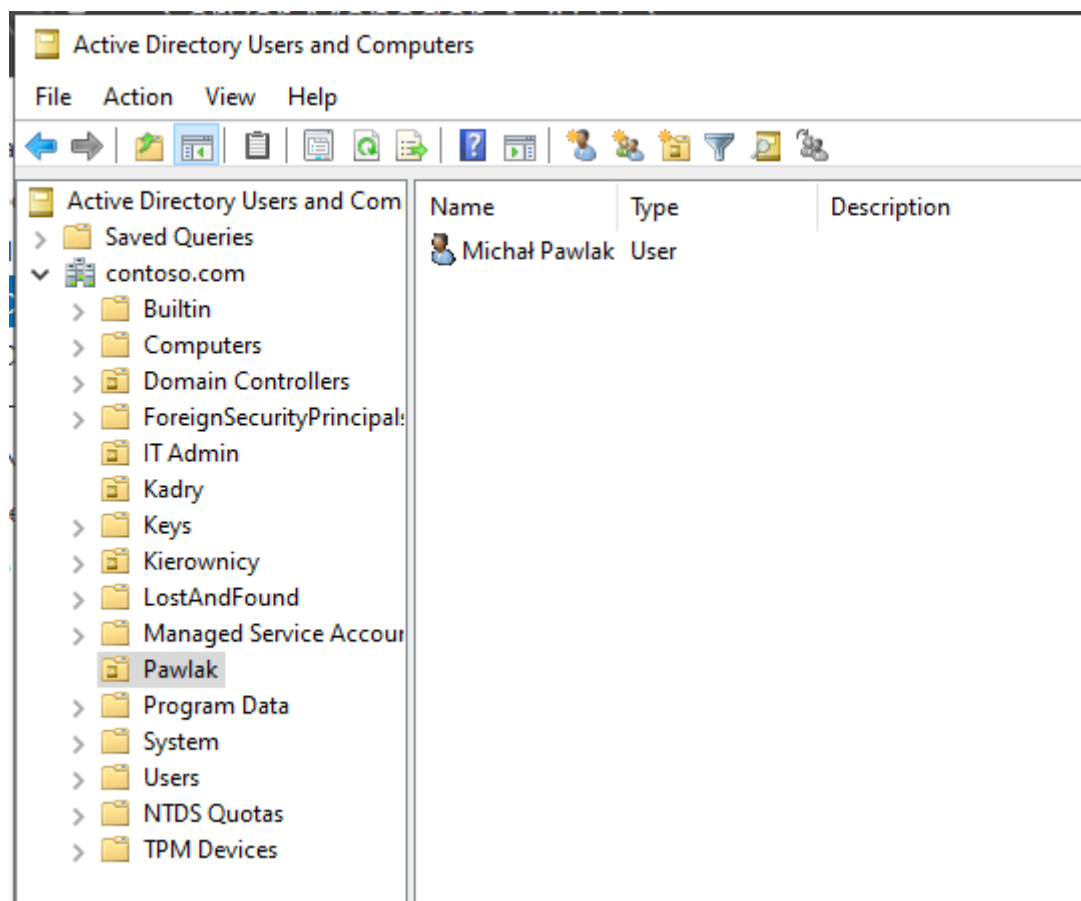
Ponadto poniżej znajduje się lista założeń, którą powinieneś wdrożyć w ramach zainstalowanego lokalnego urzędu certyfikującego:

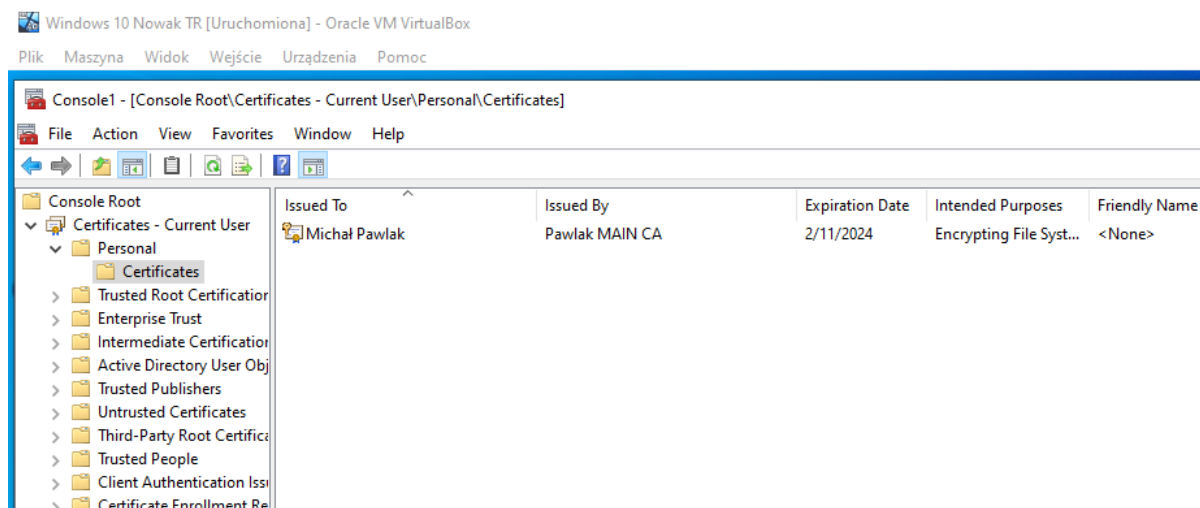
1. Utworzyć w bazie Active Directory nowego użytkownika "*Imię Nazwisko*" (gdzie pod {Imię Nazwisko} należy podstawić własne imię i nazwisko - jest to warunkiem zaliczenia sprawozdania, przykładowo: *Jan Kowalski*), a następnie zalogować się na niego w systemie Windows 8/10 i przetestować możliwość uzyskania certyfikatu dla użytkownika
2. Nadać dla użytkownika "*Imię Nazwisko*" uprawnienia do występowania o certyfikaty osobiste użytkowników w imieniu użytkowników należących do grupy *Kadry*, a następnie przetestować w systemie Windows 8/10 możliwość wystąpienia o certyfikat użytkownika w imieniu *Jacka Guli*.
3. Skonfigurować w ramach urzędu certyfikującego umieszczanie w wystawianych certyfikatach dodatkowo punktu CRL udostępnionego przez usługę http, i następnie przetestować w systemie Windows 8/10 prawidłowe działanie dokonanej konfiguracji
4. Zainstalować i skonfigurować serwer OCSP, jak również skonfigurować w ramach urzędu certyfikującego umieszczanie w wystawianych certyfikatach dodatkowo informacji o możliwości wykorzystania serwera OCSP pod odpowiednim adresem

5. Przetestować prawidłowe działanie serwera OCSP oraz listy CRL w systemie Windows 8/10
6. Na potrzeby witryny internetowej wygenerować certyfikat SSL typu multidomain wystawiony na domeny: `www.{nazwisko}.pl``www.{nazwisko}.com.pl``www.{nazwisko}.com``www.{nazwisko}.net` (gdzie pod {nazwisko} należy podstawić własne nazwisko - jest to warunkiem zaliczenia sprawozdania, przykładowo: `www.kowalski.pl`)



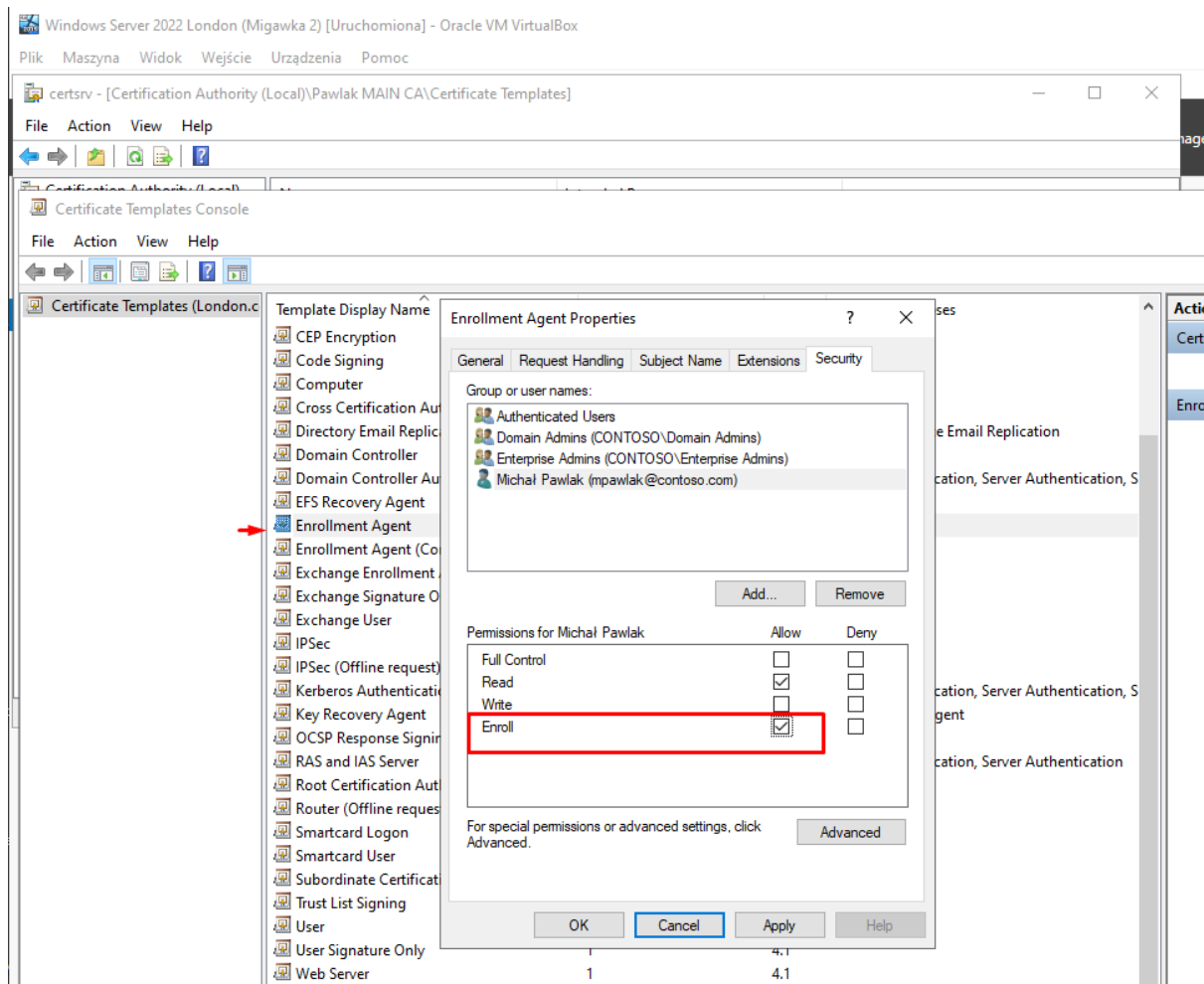
1. Utworzyć w bazie Active Directory nowego użytkownika "*Imię Nazwisko*" (gdzie pod {Imię Nazwisko} należy podstawić własne imię i nazwisko - jest to warunkiem zaliczenia sprawozdania, przykładowo: *Jan Kowalski*), a następnie zalogować się na niego w systemie Windows 8/10 i przetestować możliwość uzyskania certyfikatu dla użytkownika



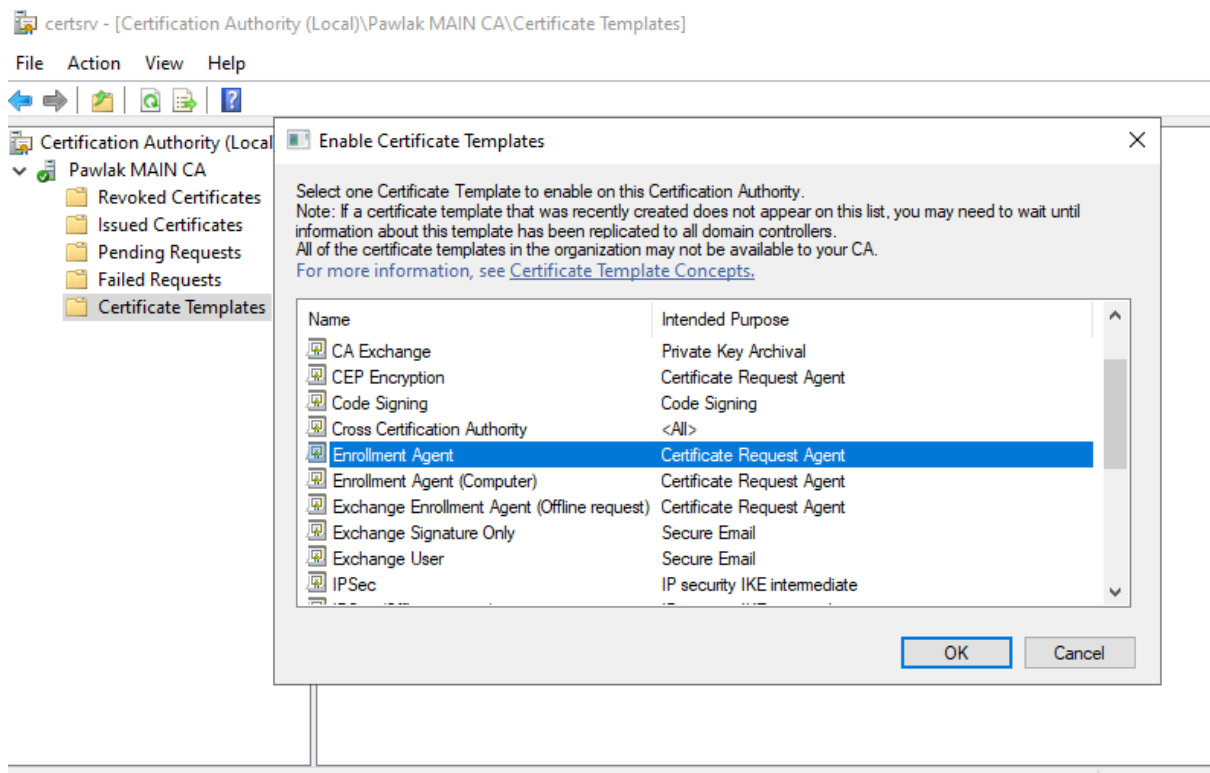


2. Nadać dla użytkownika "*Imię Nazwisko*" uprawnienia do występowania o certyfikaty osobiste użytkowników w imieniu użytkowników należących do grupy *Kadry*, a następnie przetestować w systemie Windows 8/10 możliwość wystąpienia o certyfikat użytkownika w imieniu *Jacka Guli*.

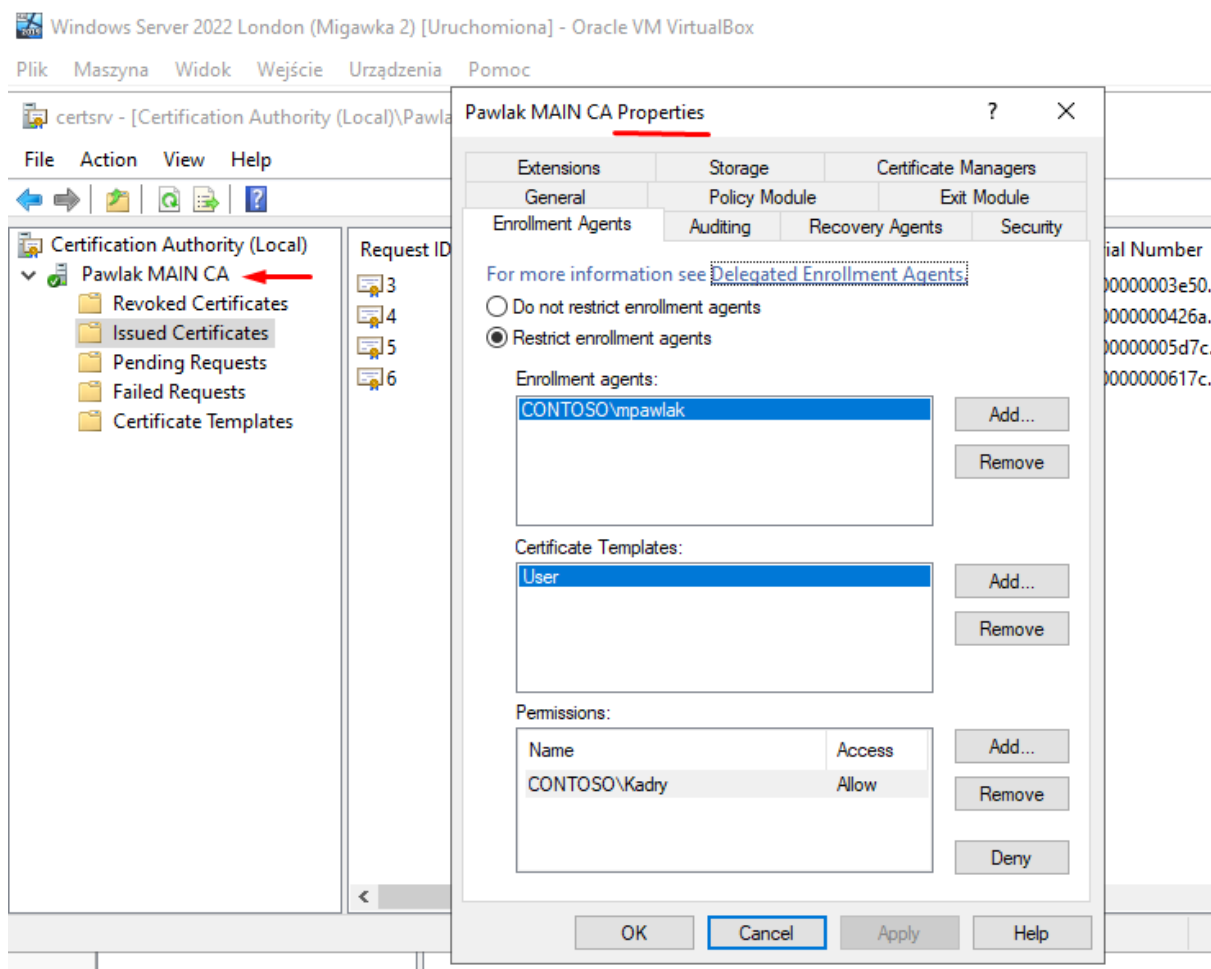
Dodanie możliwości na wystąpienie o certyfikat "Enrollment agent":



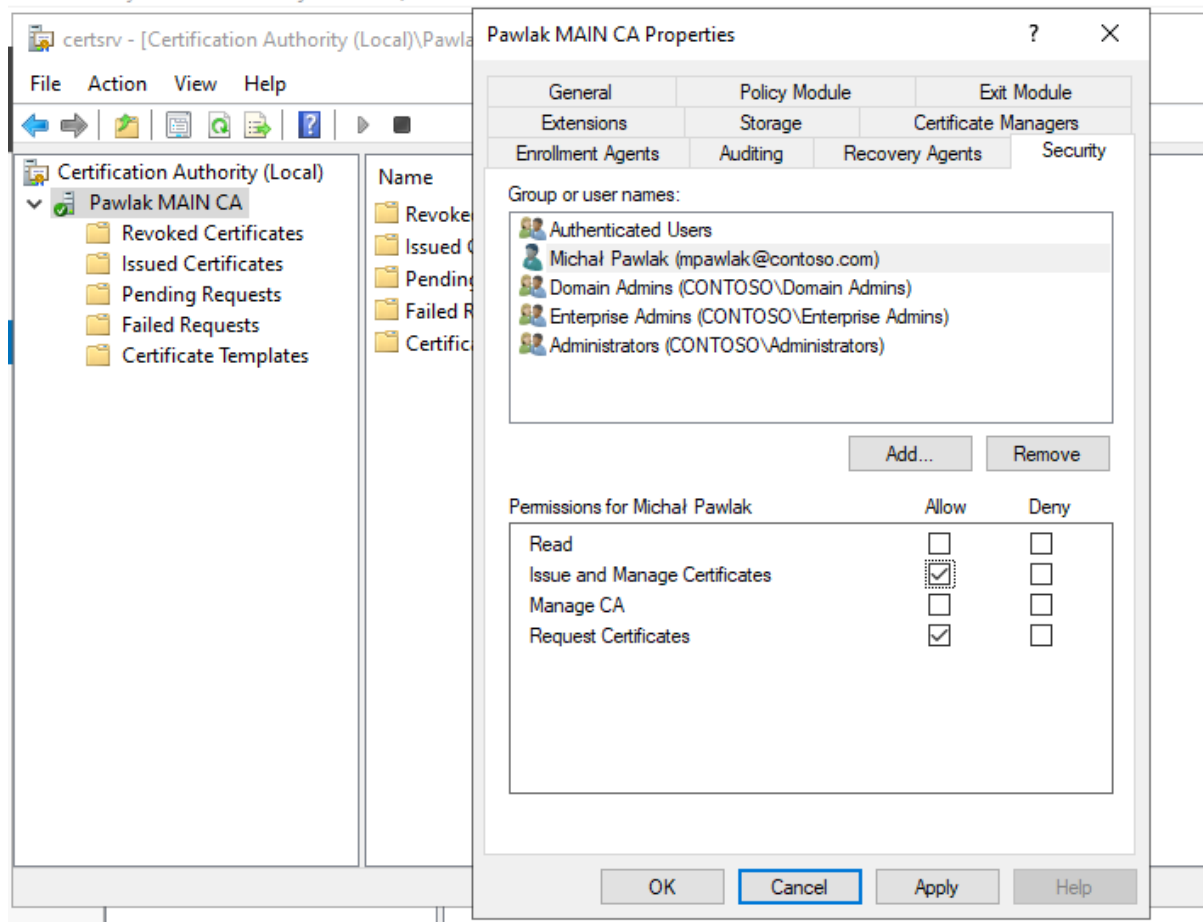
Dodanie tego wzoru certyfikatu do puli certyfikatów, o które można wystąpić:

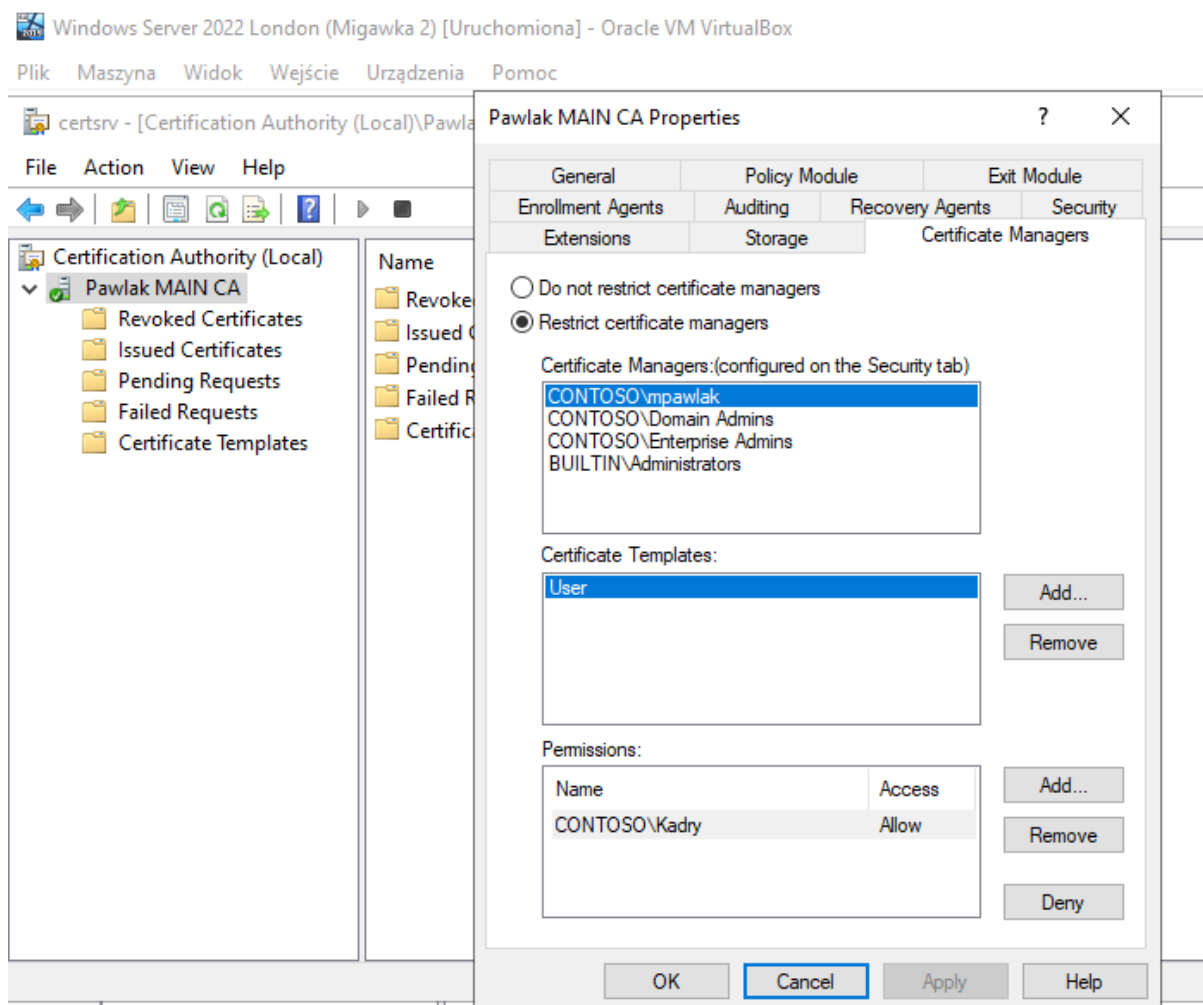


Ograniczenie roli "Enrollment Agent" dla mpawlak:

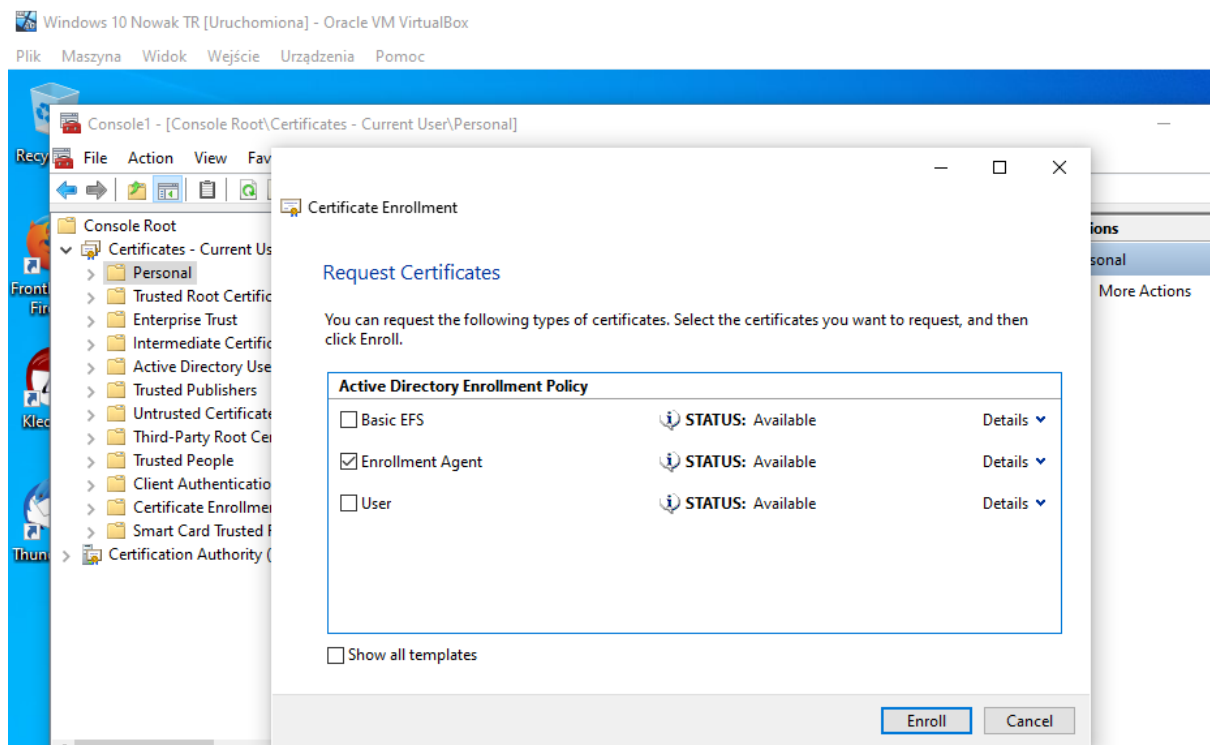


Opcjonalne: jeśli trzeba ręcznie wydawać certyfikaty, można dodać możliwość wydawania poszczególnych certyfikatów przez określone osoby:

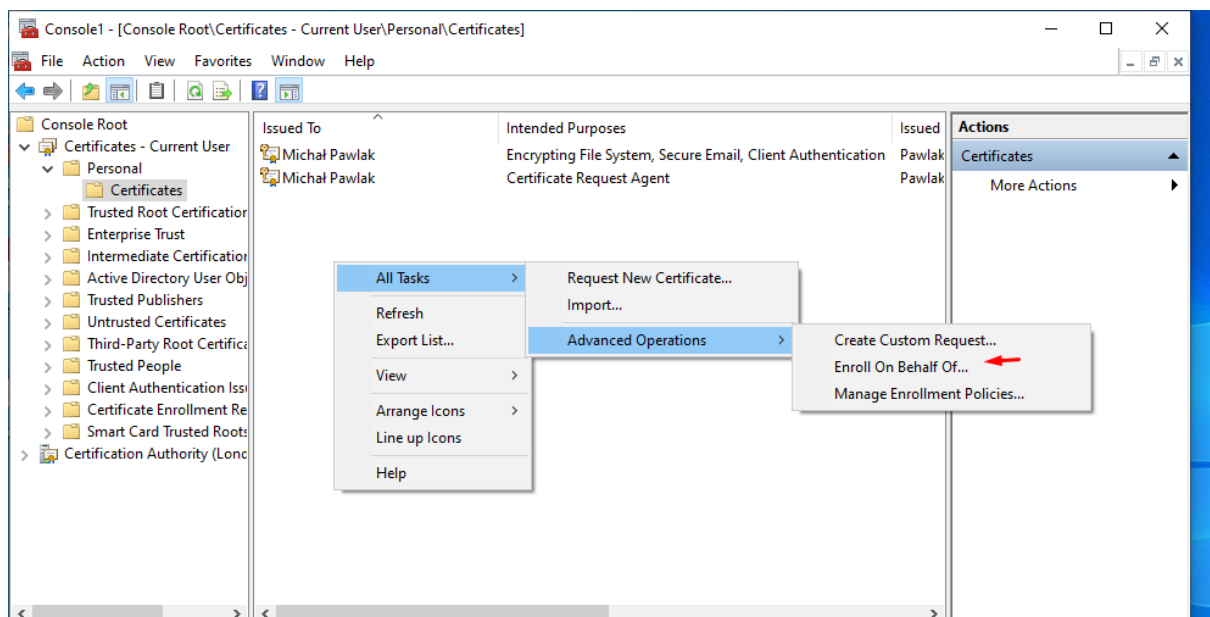




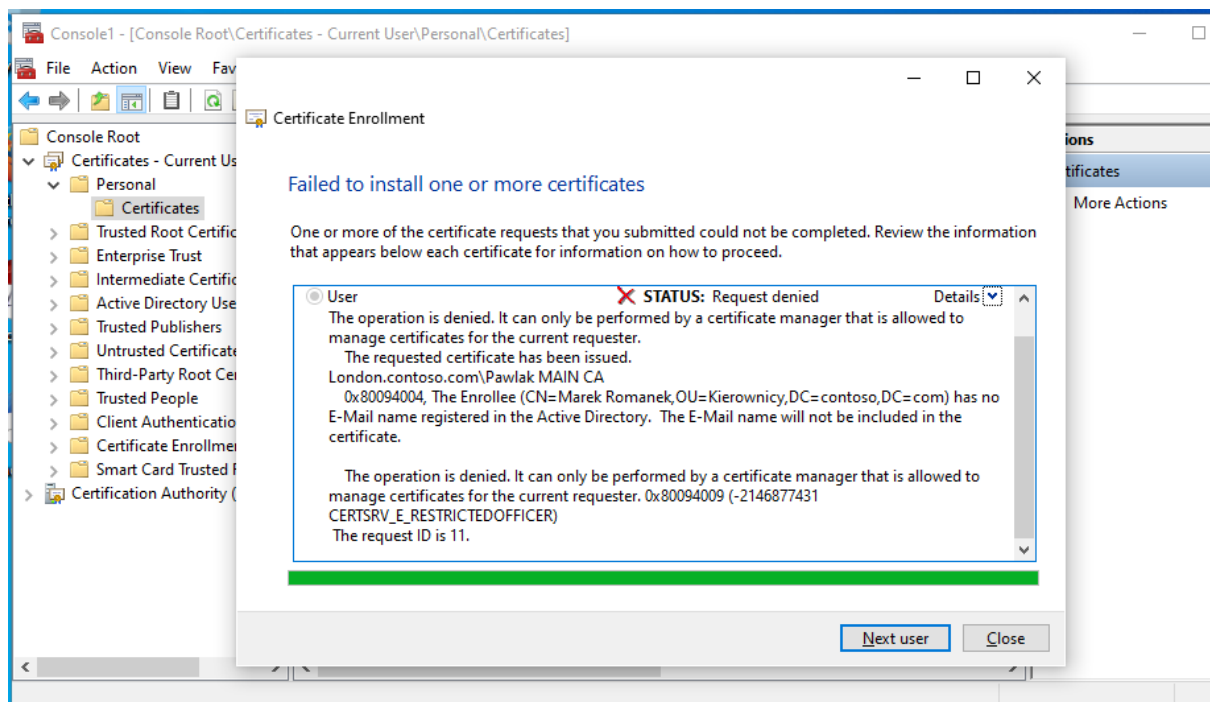
Dodanie certyfikatu "Enrollment Agent" dla mpawlak:



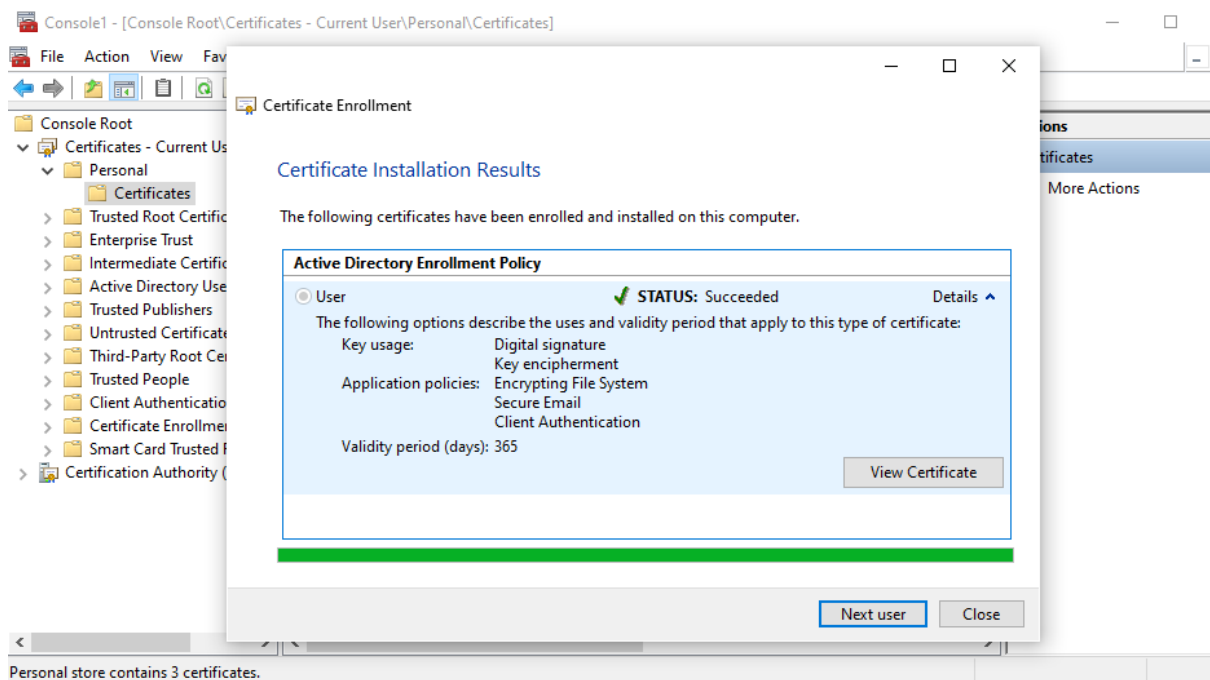
Wygenerowanie certyfikatu w imieniu innych osób:



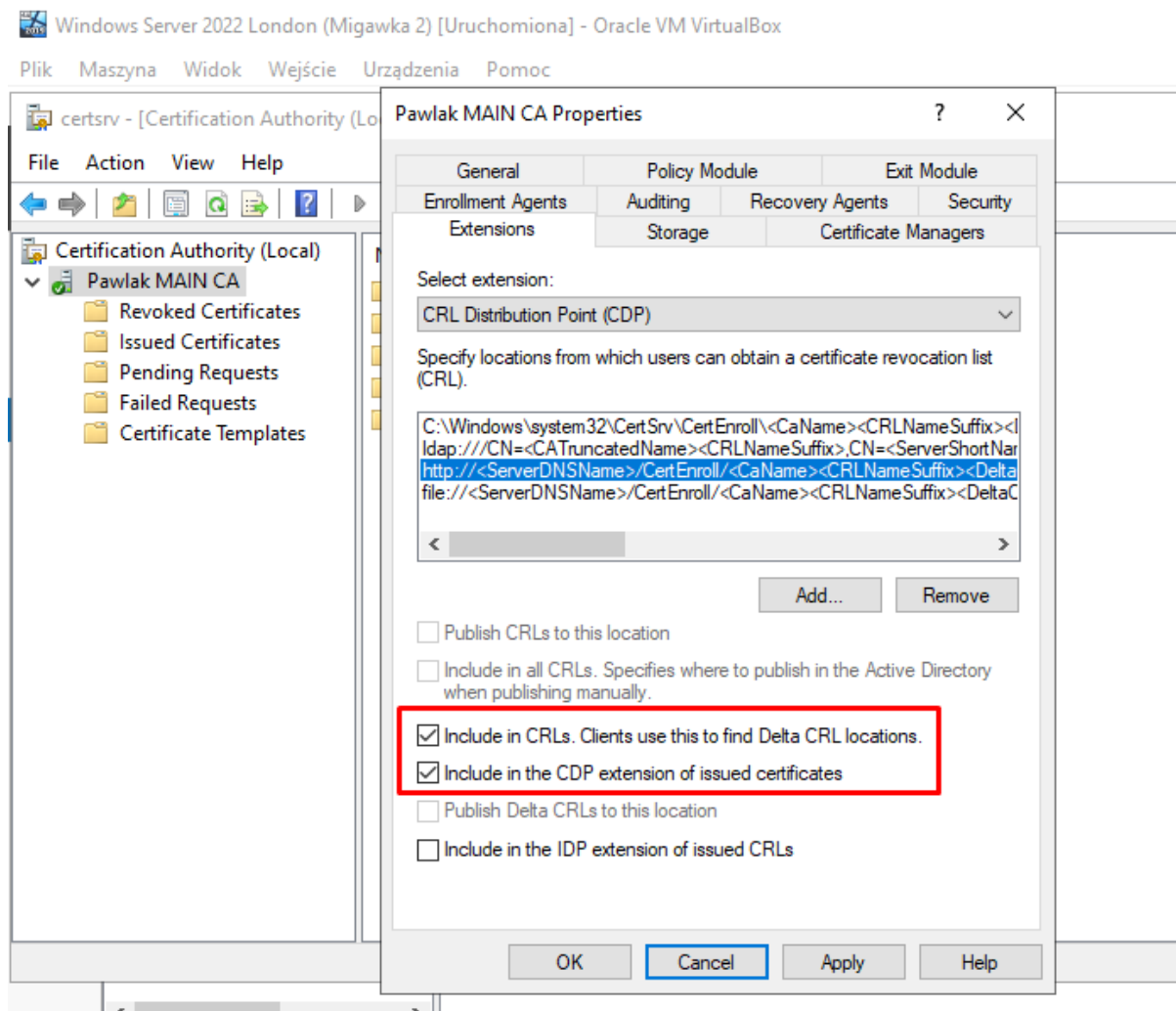
Próba wydania certyfikatu dla osobę z poza kadr:



Wydanie certyfikatu dla Jacka Guli:

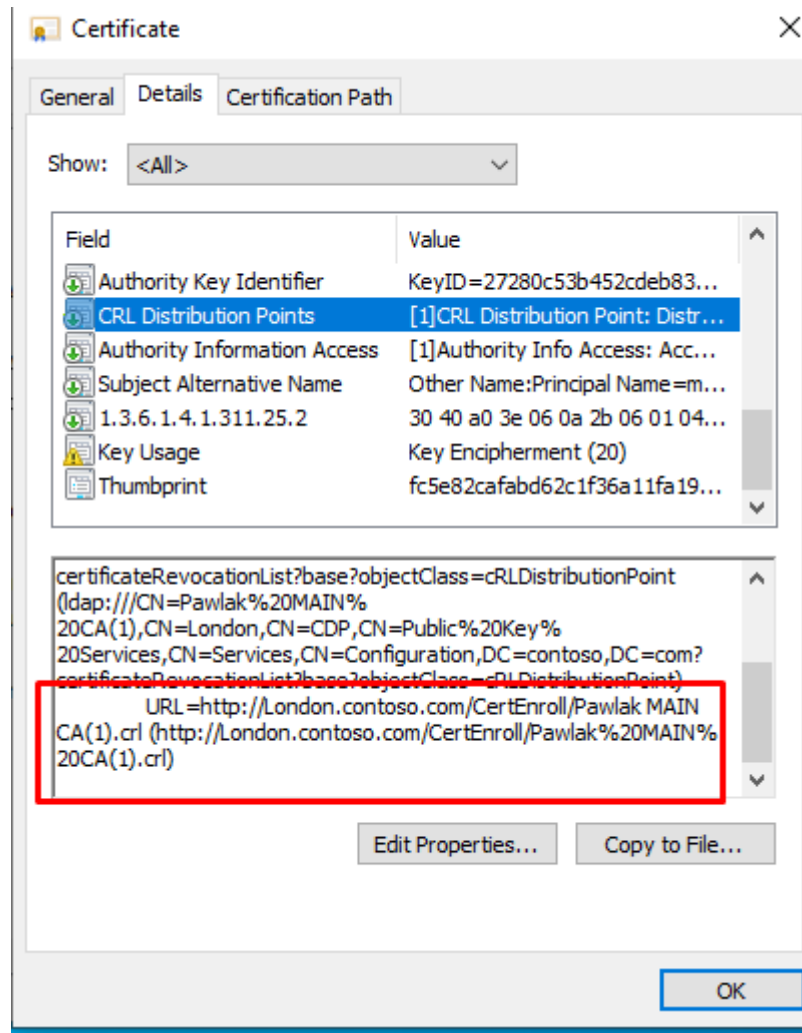


3. Skonfigurować w ramach urzędu certyfikującego umieszczanie w wystawianych certyfikatach dodatkowo punktu CRL udostępnionego przez usługę http, i następnie przetestować w systemie Windows 8/10 prawidłowe działanie dokonanej konfiguracji

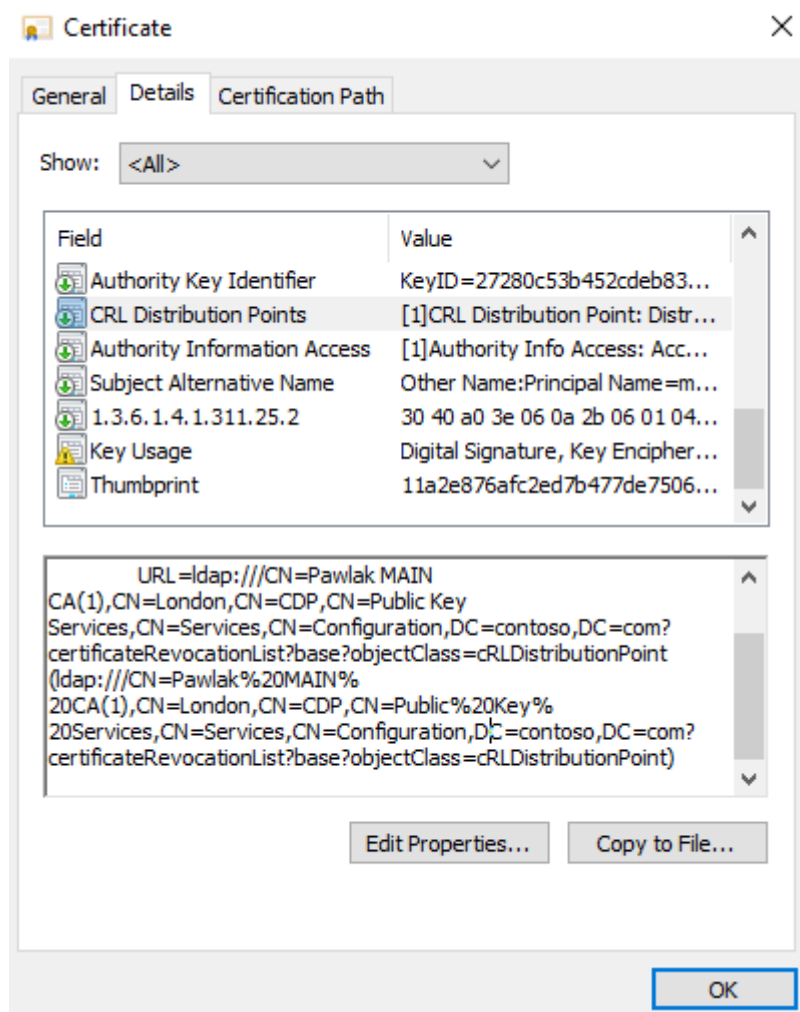


Zmiany są naniesione po restarcie usługi.

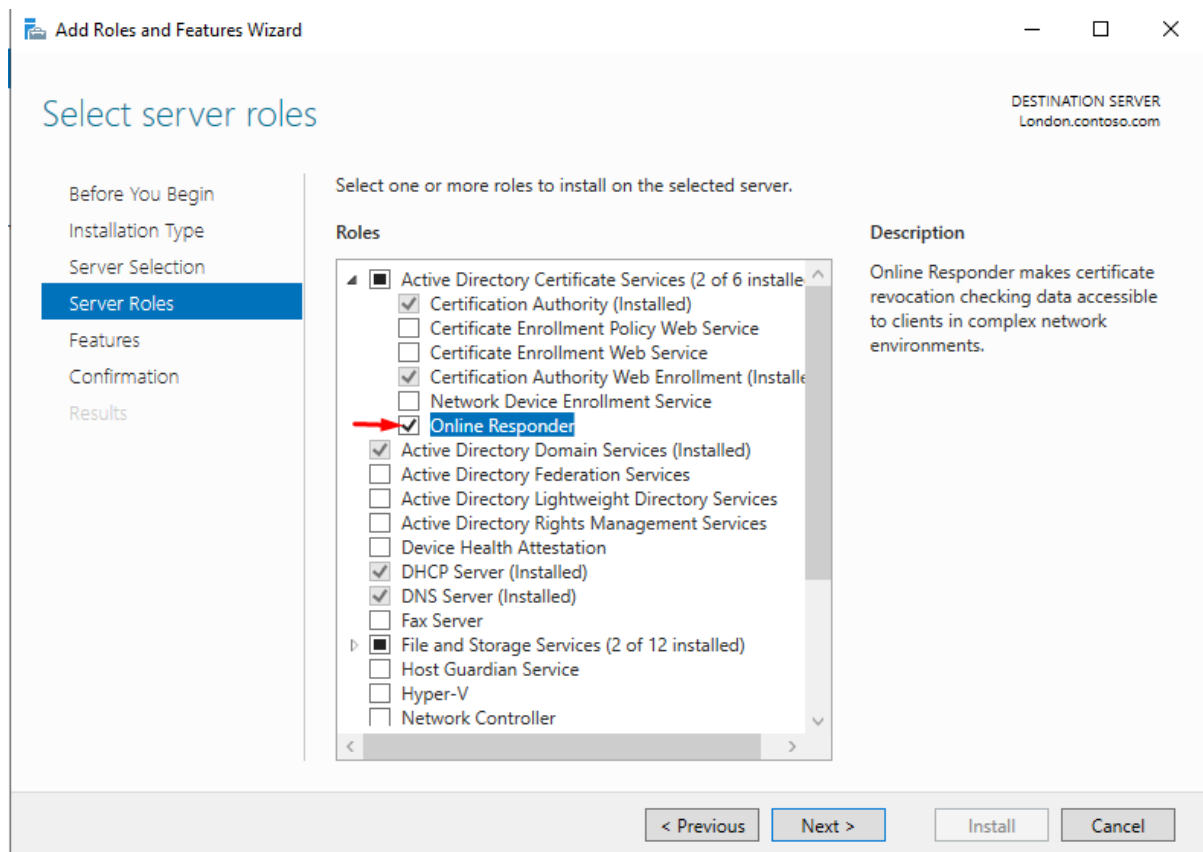
Wprowadzone zmiany będą widoczne w certyfikatach wydanych od tego momentu:



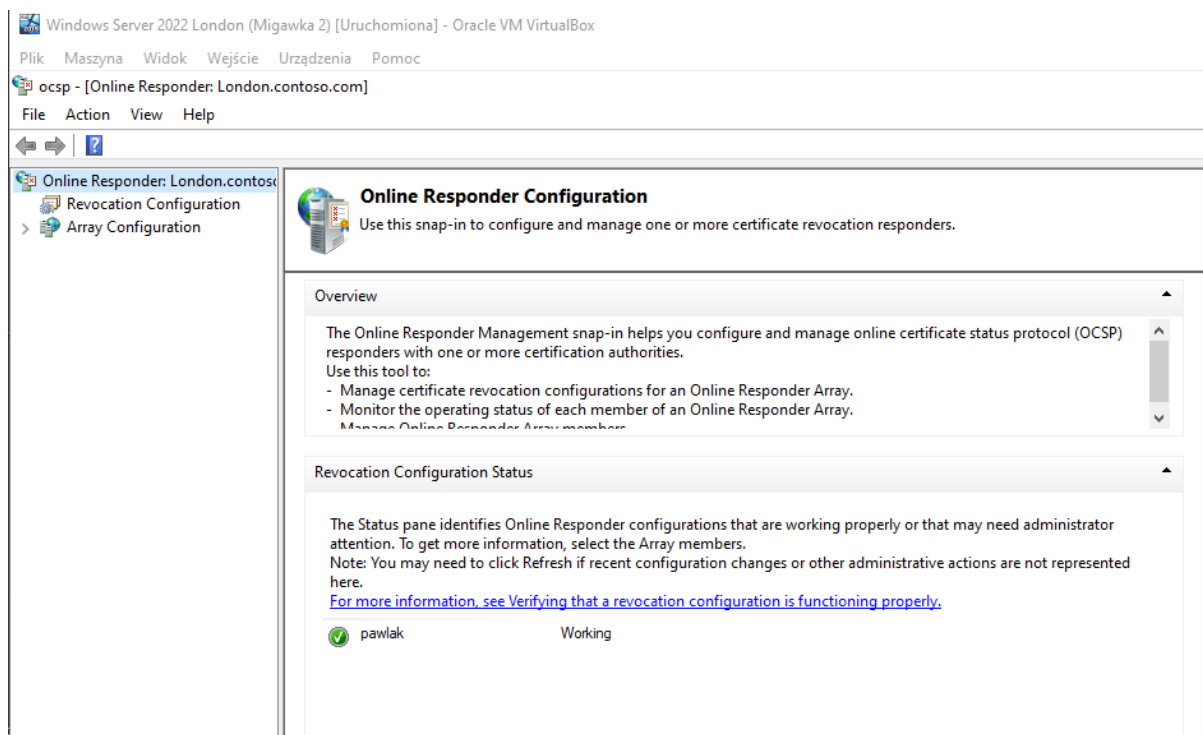
Dla porównania certyfikat z przed zmian:

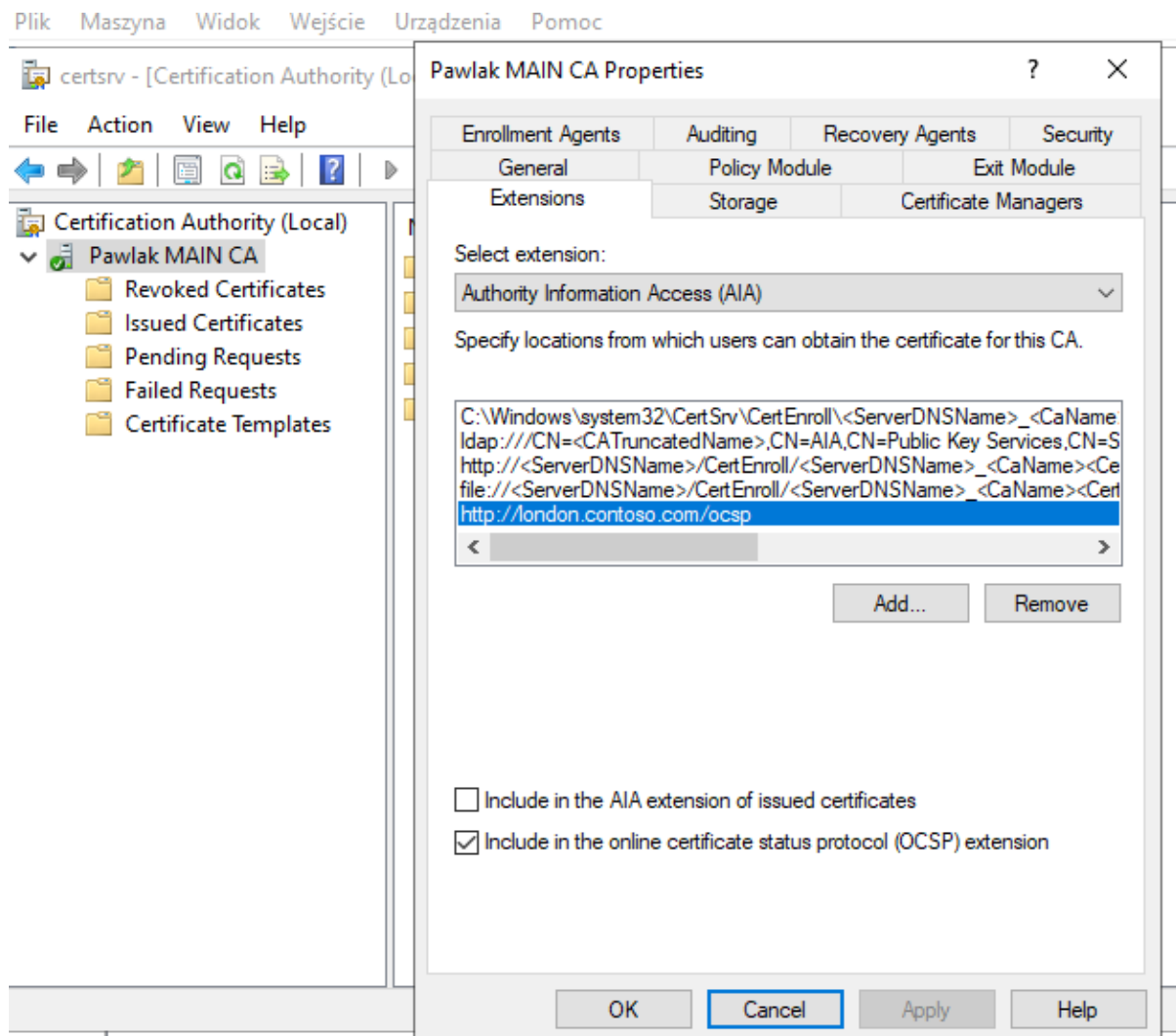


4. Zainstalować i skonfigurować serwer OCSP, jak również skonfigurować w ramach urzędu certyfikującego umieszczanie w wystawianych certyfikatach dodatkowo informacji o możliwości wykorzystania serwera OCSP pod odpowiednim adresem



Po konfiguracji:





5. Przetestować prawidłowe działanie serwera OCSP oraz listy CRL w systemie Windows 8/10

C:\Windows\system32\cmd.exe - certutil -url c:\cert\paw.cer

C:\Users\mpawlak>certutil -url c:\cert\paw.cer

URL Retrieval Tool

Status	Type	Url	Retrieval Time	Thumbprint
Verified	OCSP	[0.0] http://london.contoso.com/ocsp	0	bd511b83fe...

Timeout (sec) Note: CRLs or certificates being downloaded are not exhaustively verified. A CRL or cert may still be inconsistent or may not have the proper extensions to allow for correct verification.

☐ Sign LDAP Traffic

Certificate Subject

Retrieve
☐ Certs (from AIA)
☐ CRLs (from CDP)
☒ OCSP (from AIA)

Url to Download

C:\Windows\system32\cmd.exe - certutil -url c:\cert\paw.cer

C:\Users\mpawlak>certutil -url c:\cert\paw.cer

URL Retrieval Tool

Status	Type	Url	Retrieval Time	Thumbprint
Verified	Base CRL (...)	[0.0] ldap:///CN=Pawlak%20MAIN%2...	0	375aba81e...
Verified	Delta CRL (...)	[0.0.0] ldap:///CN=Pawlak%20MAIN...	0	3f57fbc0c6...
Verified	Base CRL (...)	[1.0] http://London.contoso.com/Cert...	0	375aba81e...
Verified	Delta CRL (...)	[1.0.0] ldap:///CN=Pawlak%20MAIN...	0	3f57fbc0c6...

Timeout (sec) Note: CRLs or certificates being downloaded are not exhaustively verified. A CRL or cert may still be inconsistent or may not have the proper extensions to allow for correct verification.

☐ Sign LDAP Traffic

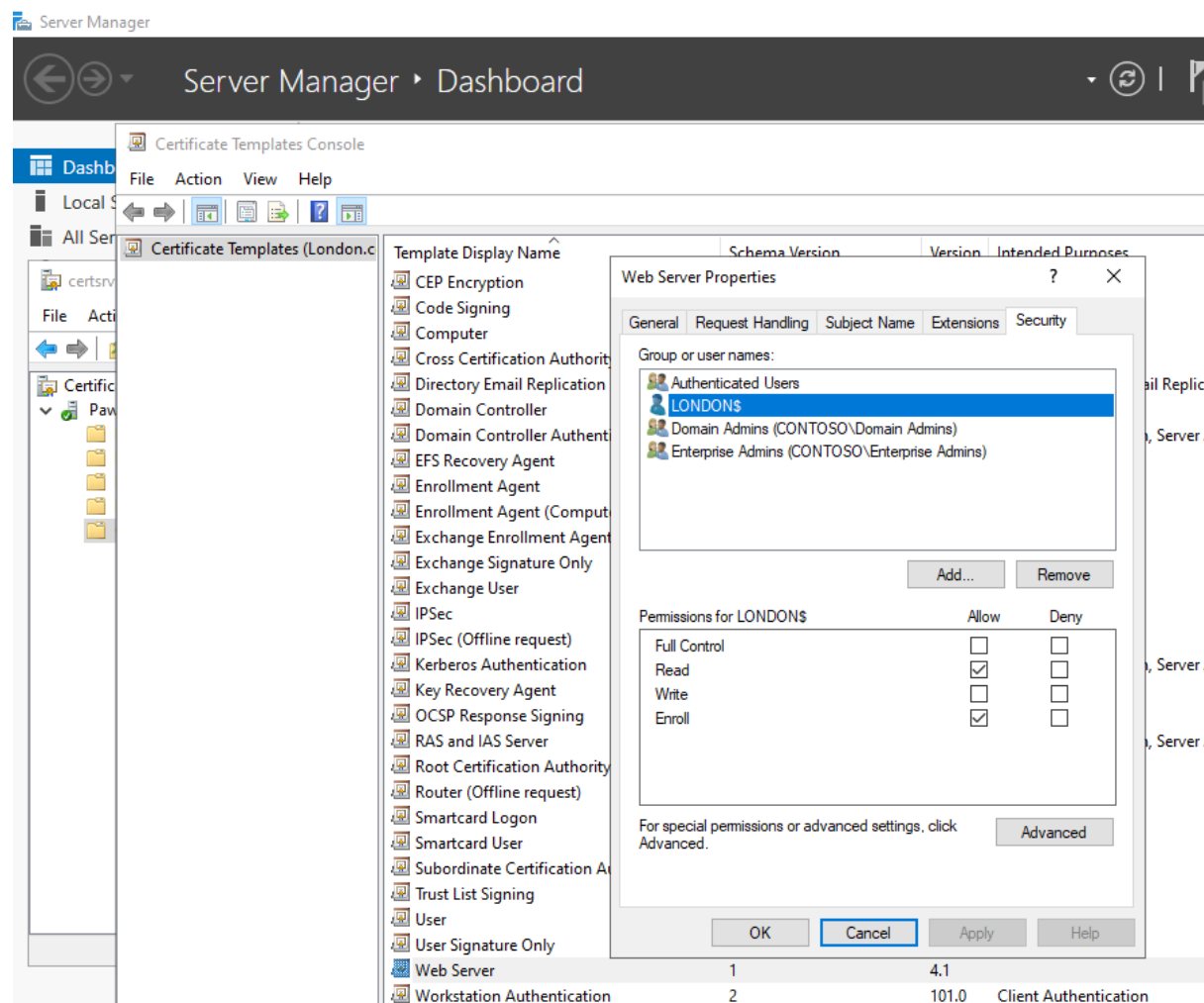
Certificate Subject

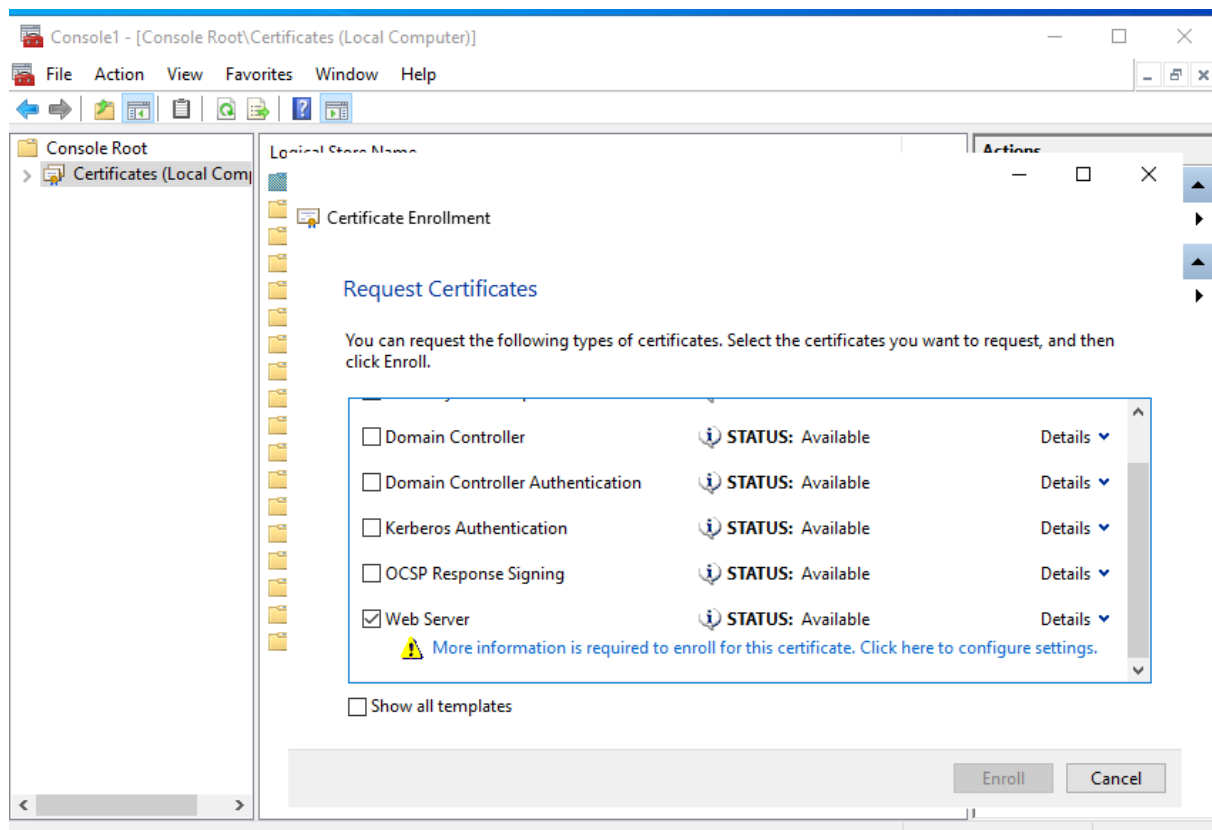
Retrieve
☐ Certs (from AIA)
☒ CRLs (from CDP)
☐ OCSP (from AIA)

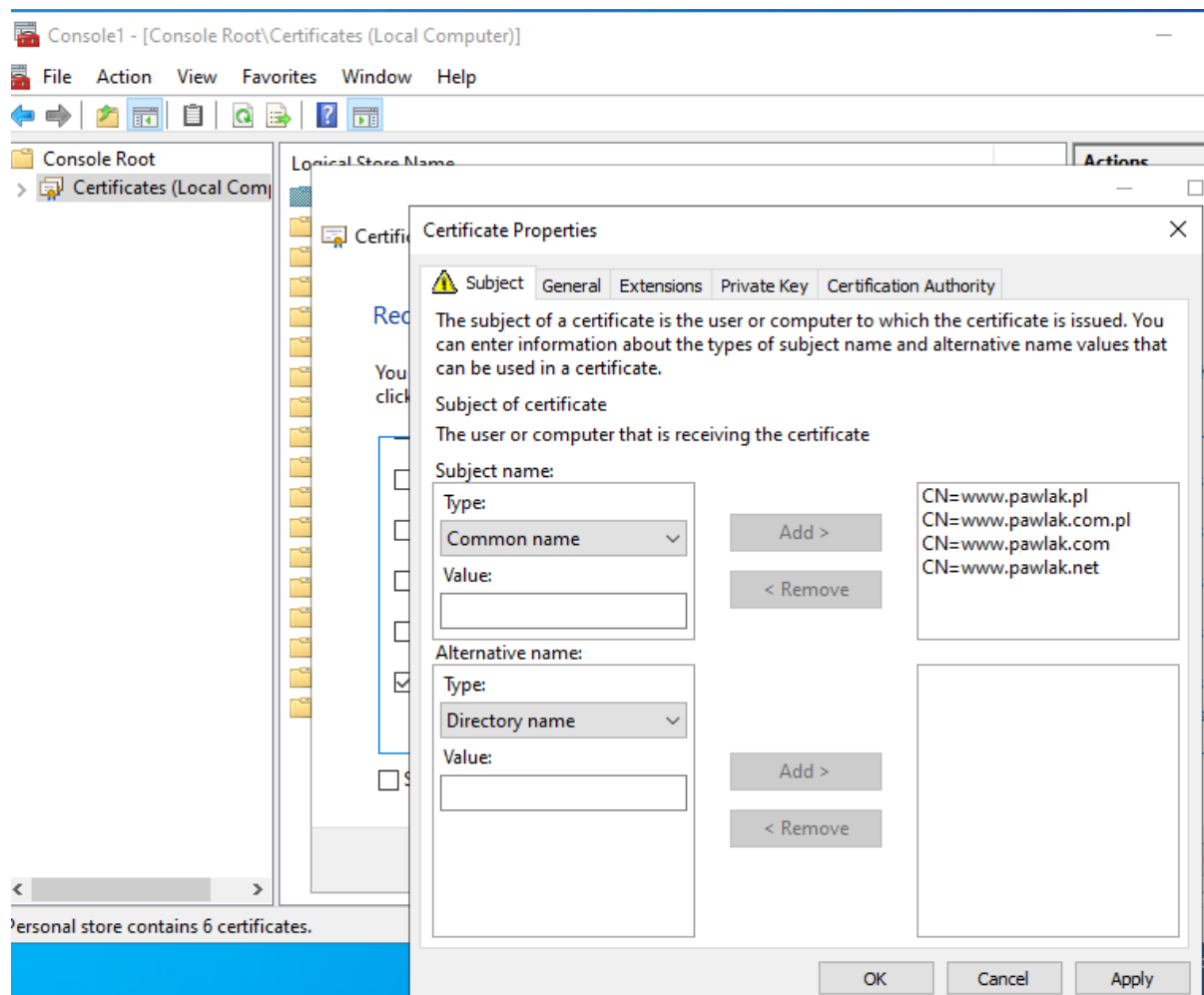
Url to Download

6. Na potrzeby witryny internetowej wygenerować certyfikat SSL typu multidomain wystawiony na domeny: www.{nazwisko}.pl www.{nazwisko}.com.pl www.


{nazwisko}.com www.{nazwisko}.net (gdzie pod {nazwisko} należy podstawić własne nazwisko - jest to warunkiem zaliczenia sprawozdania, przykładowo: *www.kowalski.pl*)







Certificate Properties ✕

 Subject General Extensions Private Key Certification Authority

A friendly name and description will make it easier to identify and use a certificate.

Friendly name:

pawlak

Description:

OK Cancel Apply

