Настройка аутентификации с помощью Рутокен ЭЦП и PKI в сети VPN на Cisco ASA

- Общая информация
- Настройка УЦ
- Настройка Cisco ASA
  - Первичная настройка
  - Получение корневого сертификата УЦ и сертификата ASA
  - Настройка VPN на ASA
- Настройка клиента VPN в Windows (AnyConnect)
- Настройка клиента VPN в Linux (OpenConnect)

Общая информация

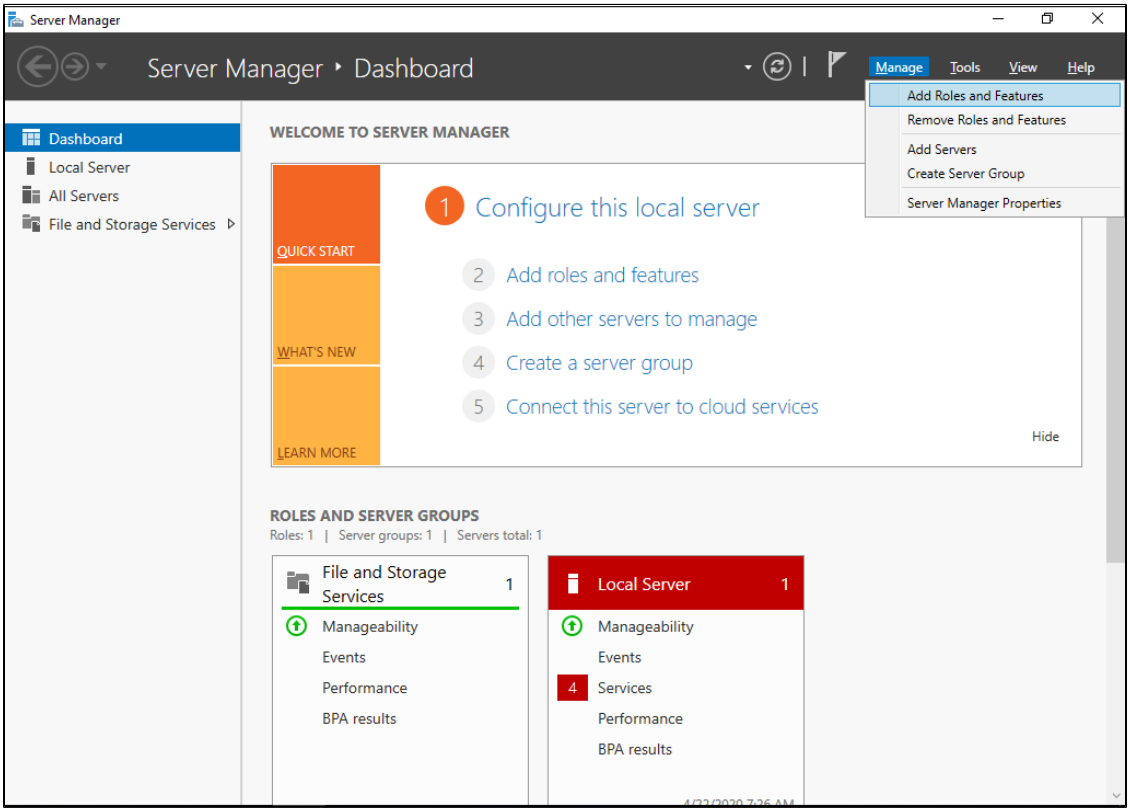
Для создания сети VPN и настройки аутентификации в ней нам понадобится:

- Cisco ASA (в нашем случае будет использована виртуальная машина ASAv, эмулирующая его работу).
- Сервер с УЦ (в нашем случае будет использован WIndows Server с установленным и настроенным на нем Active Directory Certificate Services).
- Клиент для подключения к сети VPN (в нашем случае это будет AnyConnect на Windows и OpenConnect на Linux).

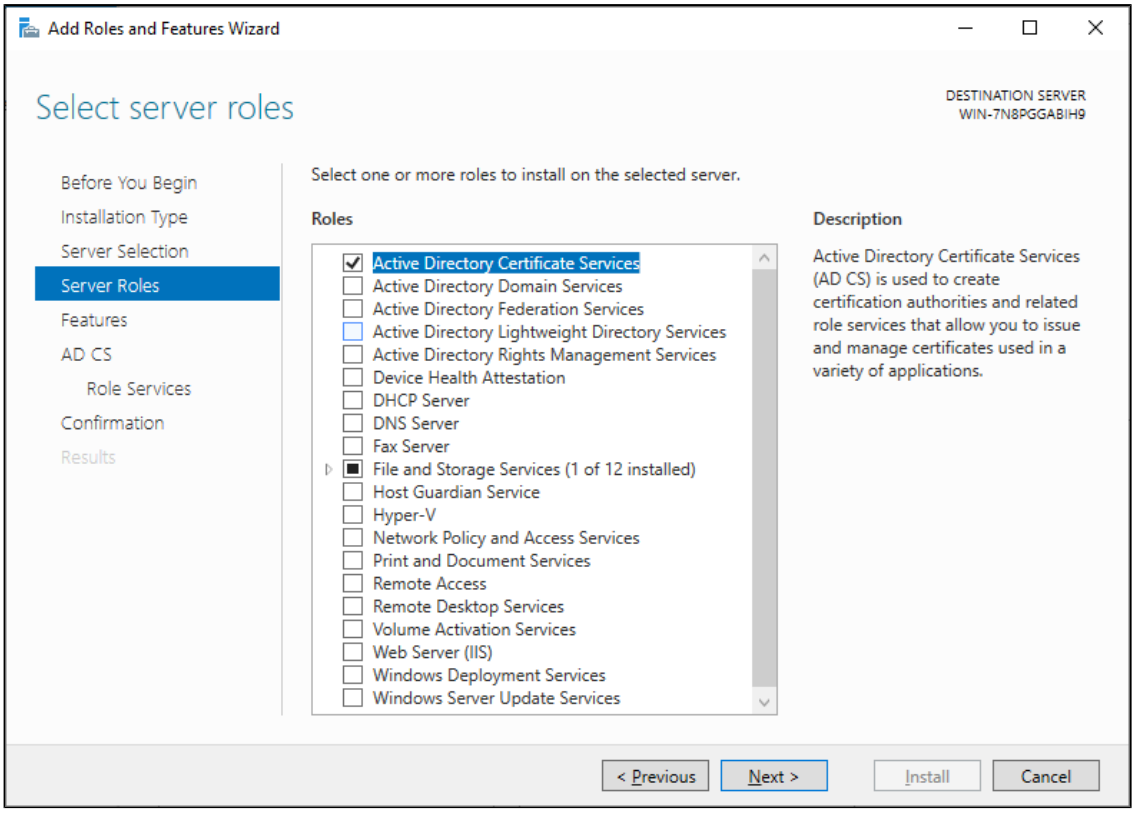
Настройка УЦ

Для начала настроим наш УЦ, который расположен у нас на Windows Server. Чтобы развернуть УЦ необходимо через "Server Manager" поставить "Active Directory Certificate Services". Для этого:

Нажимаем на "Manage"->"Add Roles and Features"

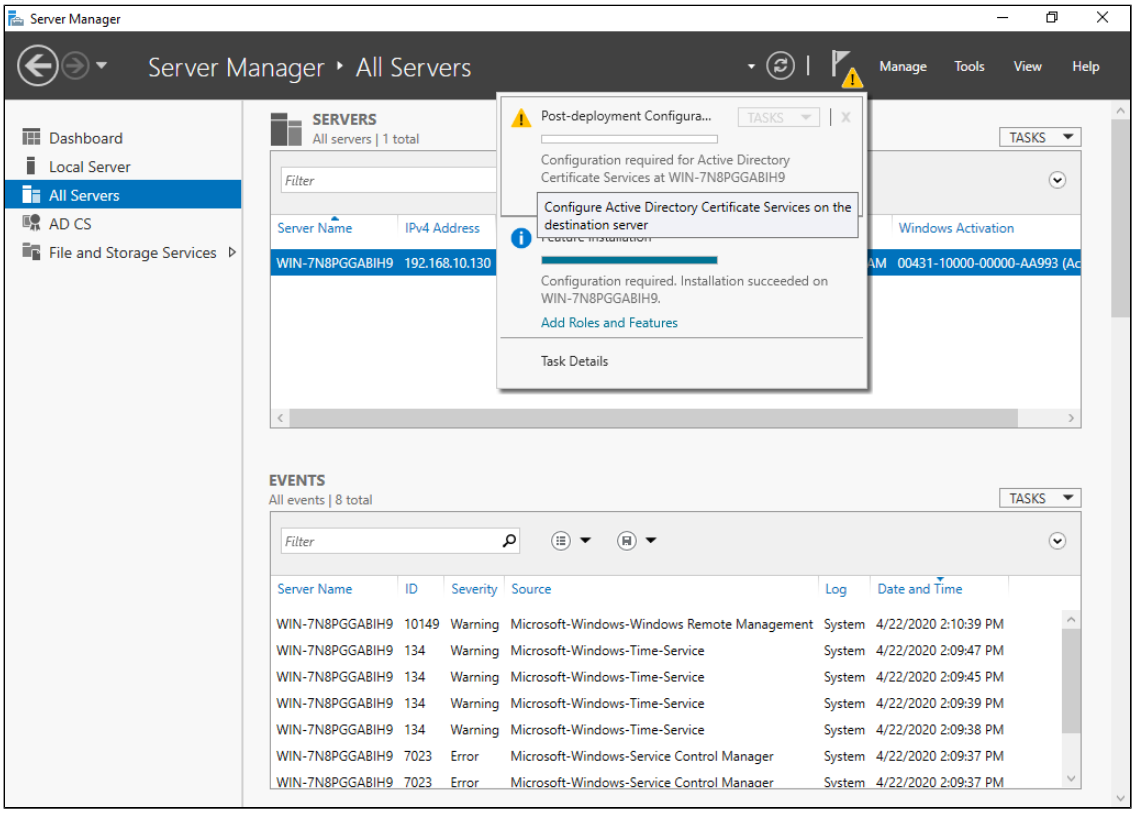


Переходим на вкладку "Server Roles" и выбираем "Active Directory Certificate Services"

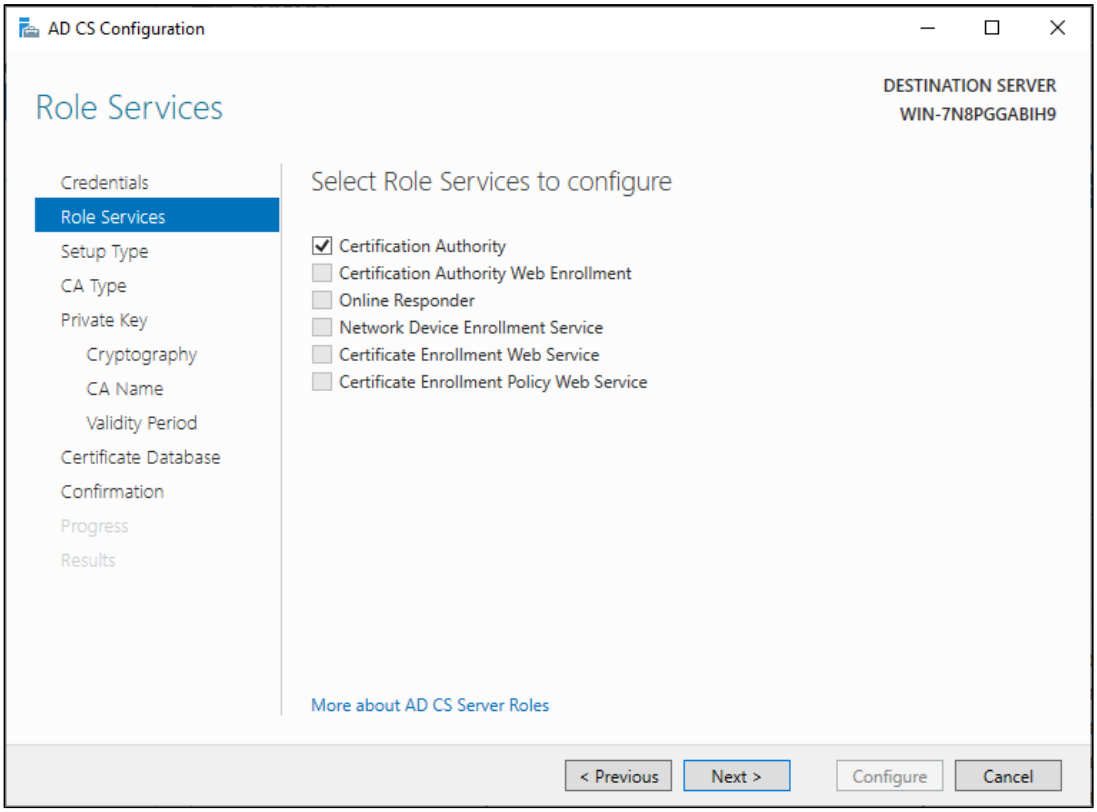


На всех остальных вкладках нажимаем "Next".

После установки настраиваем наш УЦ. Для этого нажимаем на значок уведомления и выбираем вкладку "Configure Active Directory Certificate Services"

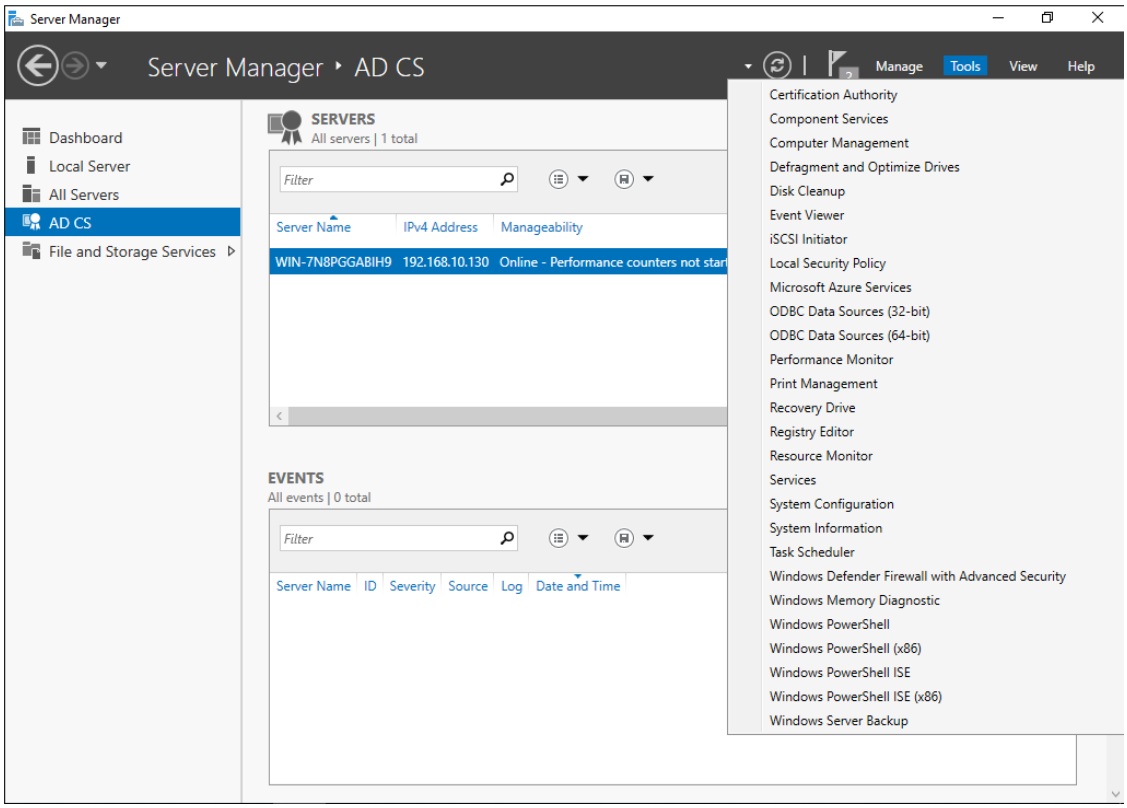


На второй вкладке установите галочку "Certification Authority"



На всех остальных вкладках нажимаем "Next".

Далее откроем программу для управления УЦ, для этого выбираем "AD CS"->"Tools"→"Certification Authority".

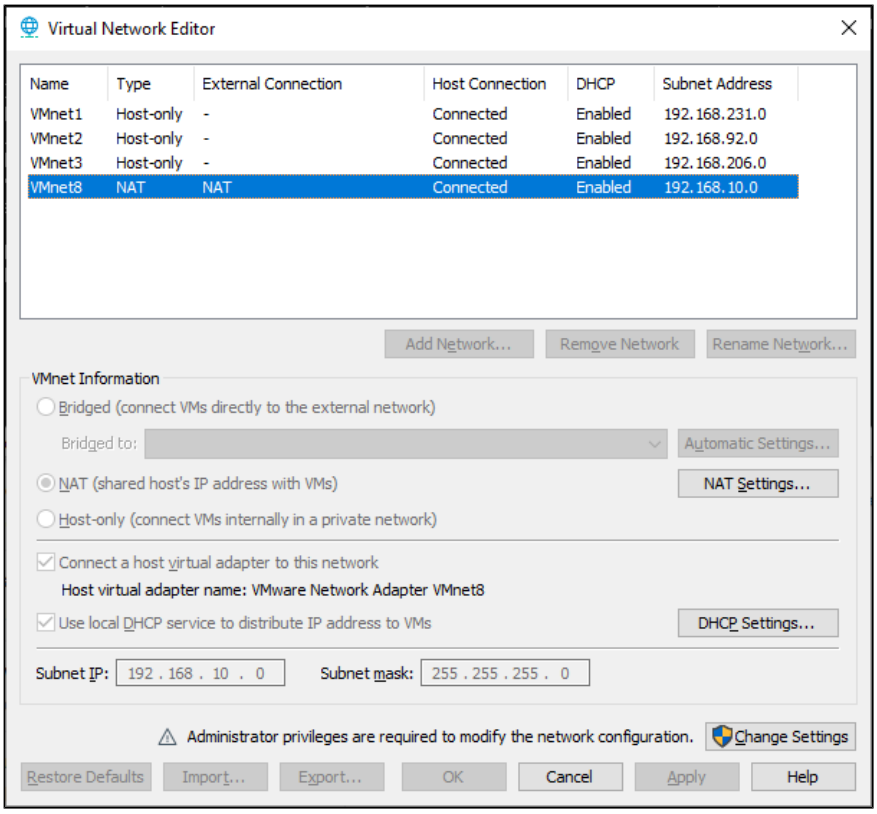


Настройка Cisco ASA

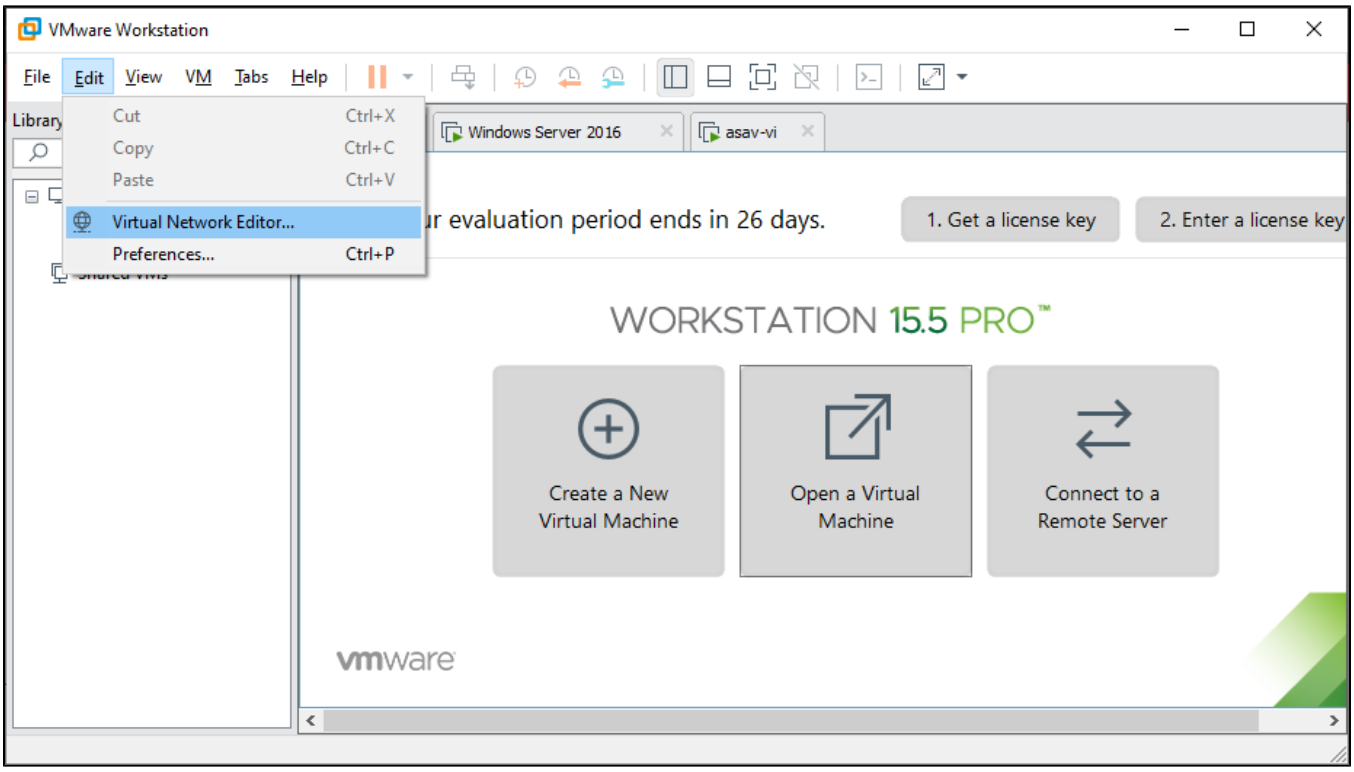
Первичная настройка

Теперь приступим к настройке Cisco ASA. Для упрощения процесса настройки, все действия будем производиться через Cisco ASDM. Это графическое приложение для управление ASA.

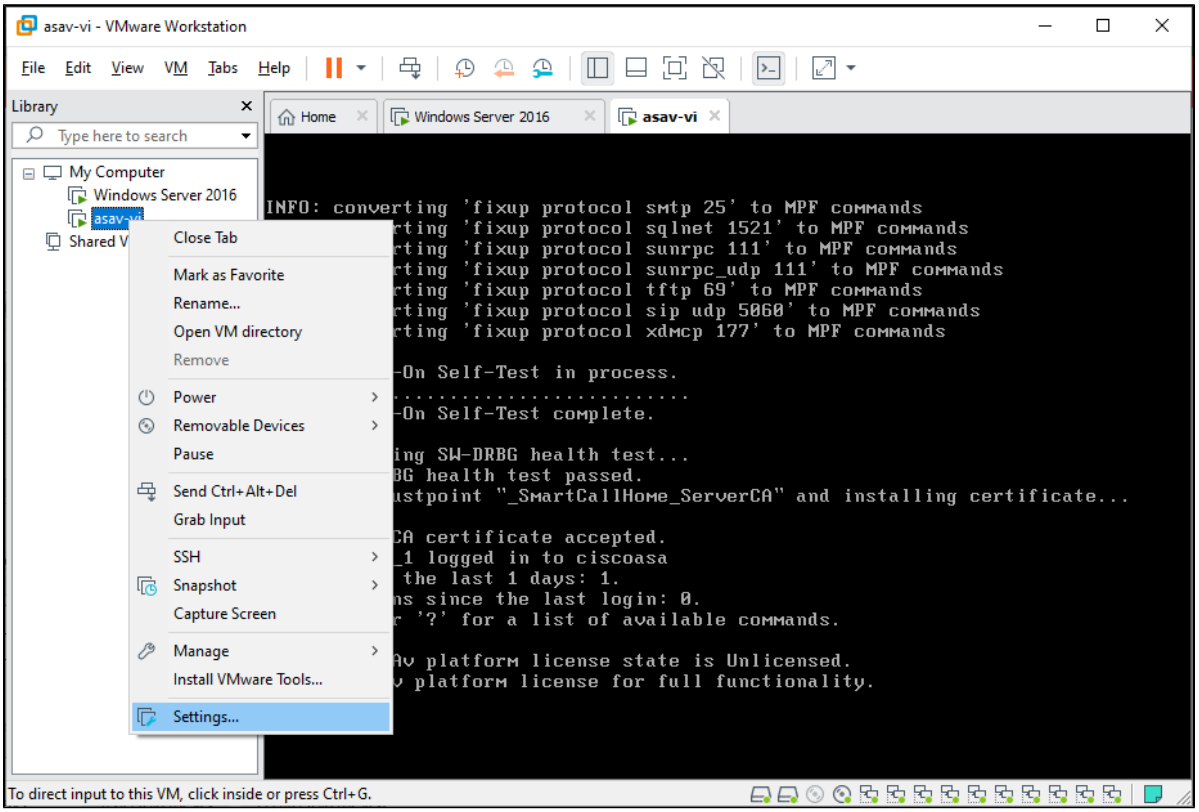
Для подключения через ASDM, подключим управляющий интерфейс в одну сеть с нашим компьютером, на котором установлен "ASDM". В нашем случае данной сетью будет являться VMnet8 (192.168.10.0/24).

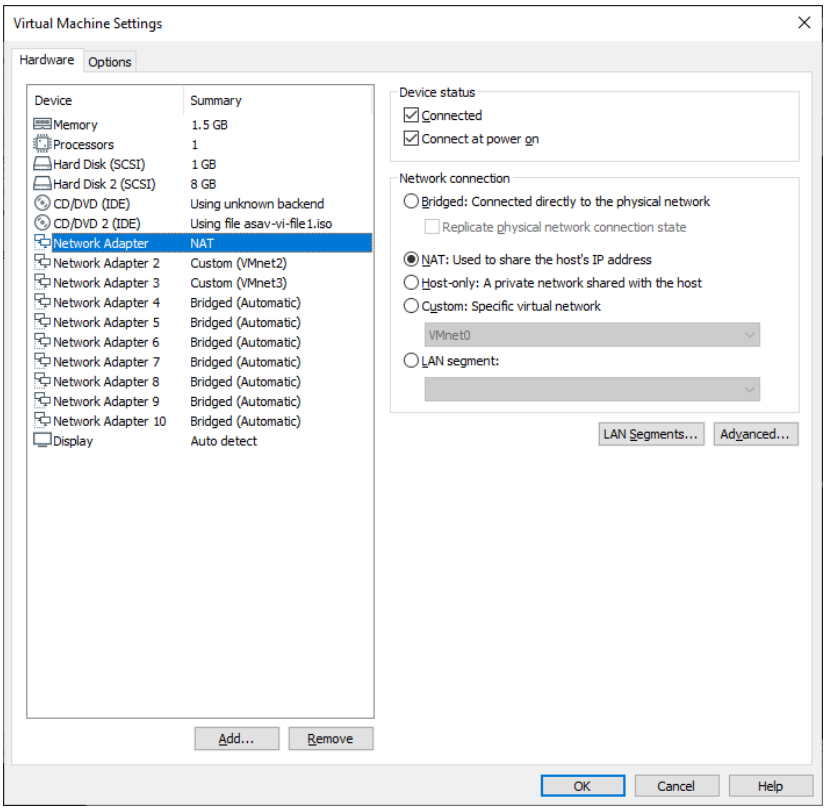


В VMware узнать адрес данной сети можно через вкладку "Edit"→"Virtual Network Editor...".



Подключить управляющий интерфейс к данной сети можно через настройки виртуальной машины.



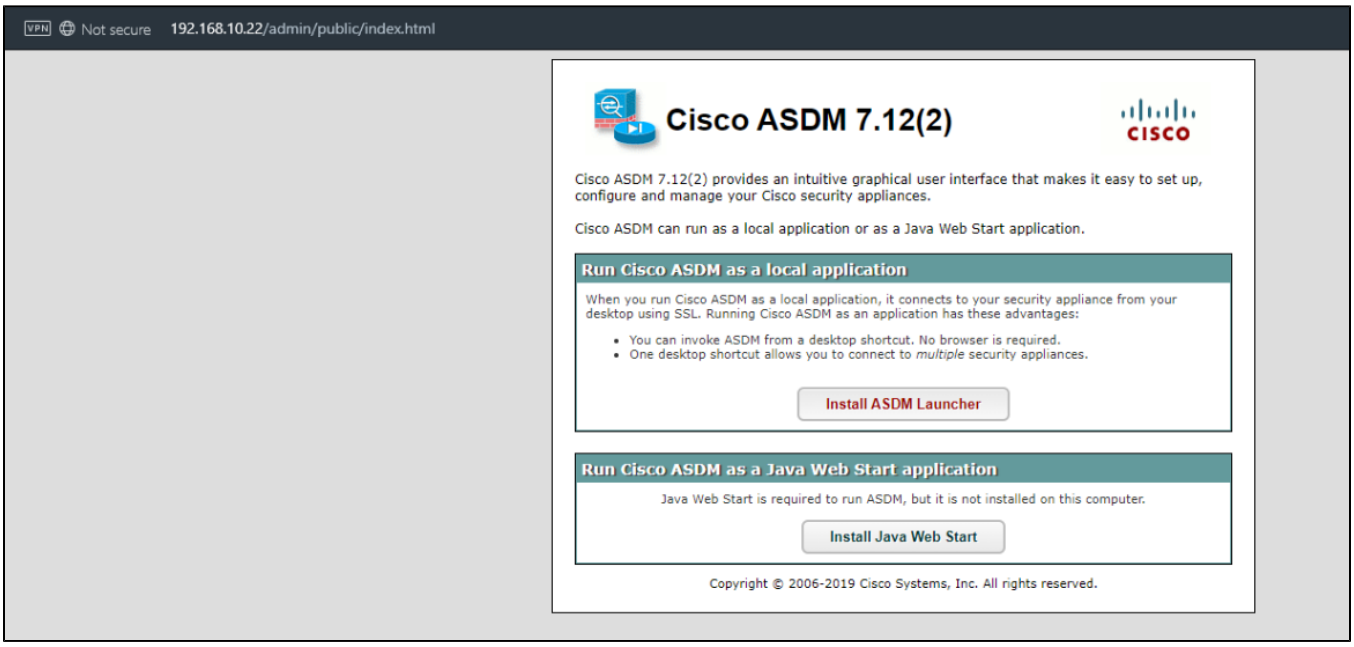


Теперь зададим статический IP-адрес для данного интерфейса в нашем МЭ. Для этого выполним следующую последовательность команд:

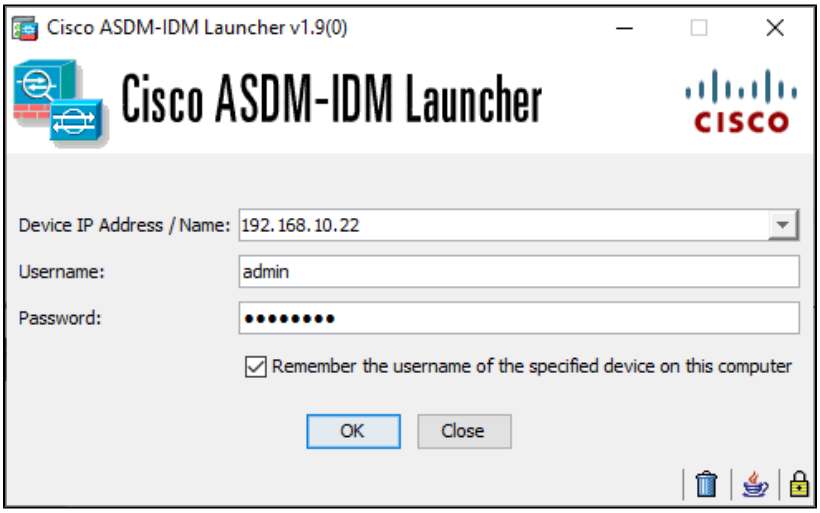
Первичная настройка Cisco ASA

```
ciscoasa> en
#
ciscoasa# conf t
ciscoasa(config)# int management 0/0
ciscoasa(config-if)# ip add 192.168.10.22 255.255.255.0
ciscoasa(config-if)# nameif mgmt
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
ciscoasa(config)# http server enable
ciscoasa(config)# http 0 0 mgmt
#
ciscoasa(config)# username <admin_name> password <password> privilege 15
ciscoasa(config)# wr
```

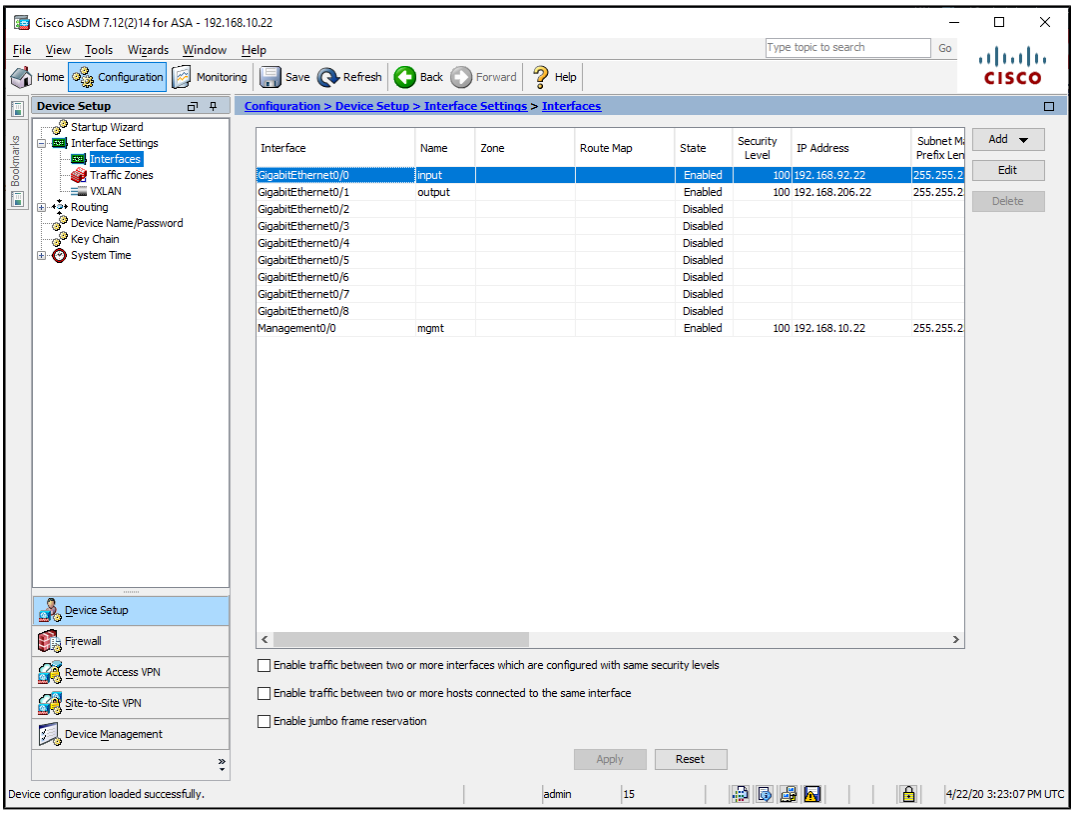
После этого через браузер нашего клиента подключимся к запущенному веб-серверу ASA. В нашем случае подключаемся по адресу https://192.168.10.22/. Установить ASDM можно на этой страницы.



Запустим ASDM и подключимся к МЭ.

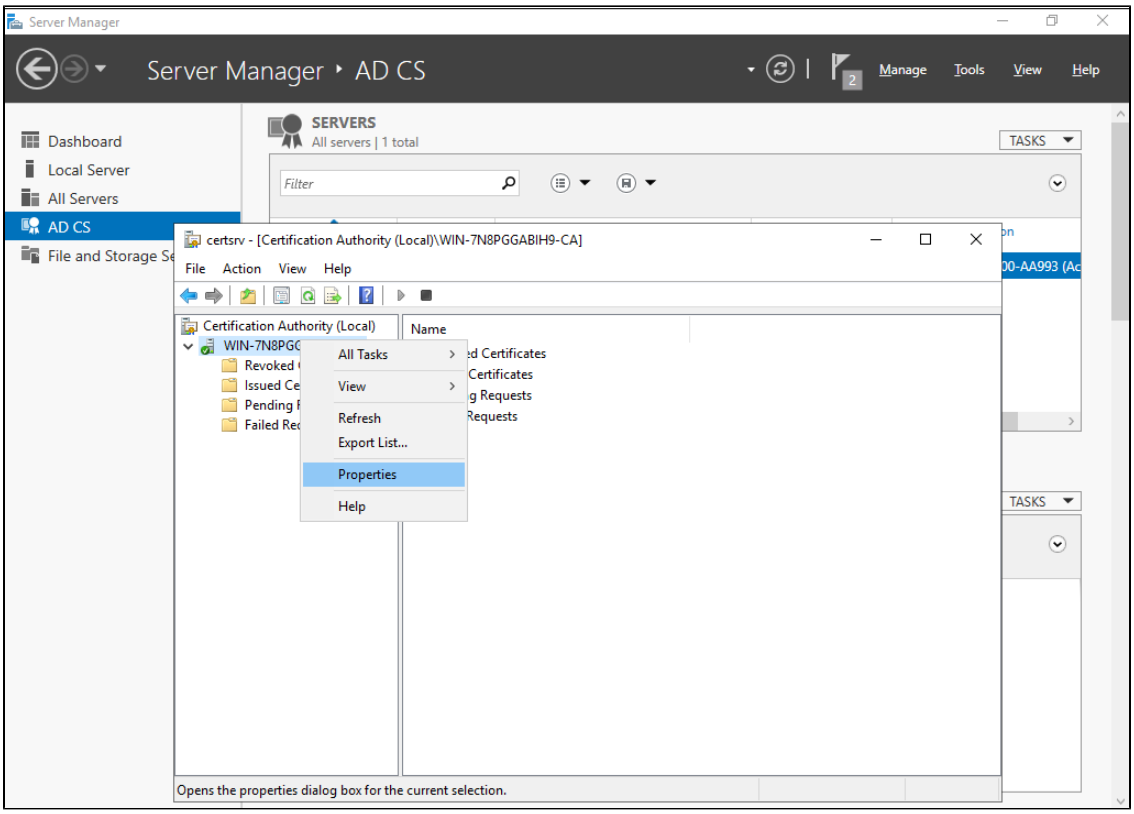


Через данный графический менеджер можно настроить оставшиеся входные и выходные интерфейсы МЭ. Это можно сделать на вкладке "Configuration"→"Interface settings"→"Interfaces":

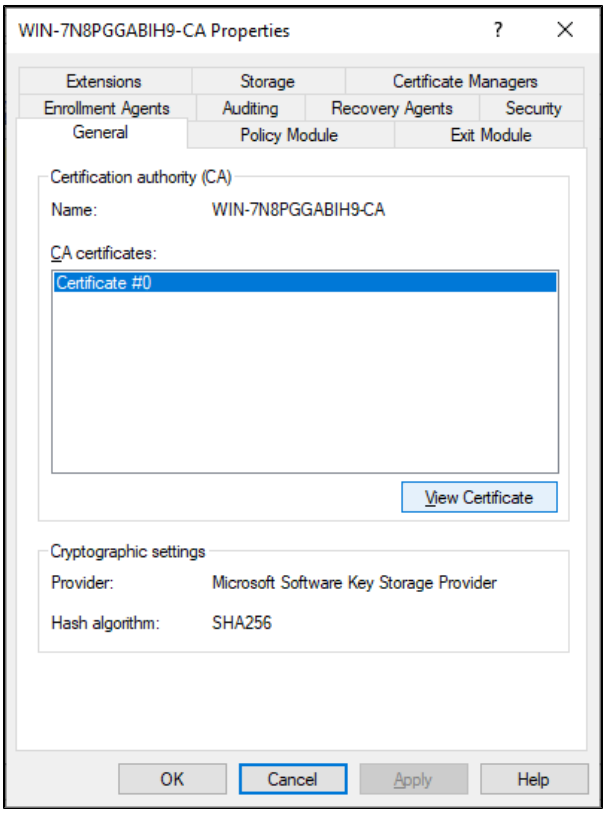


Получение корневого сертификата УЦ и сертификата ASA

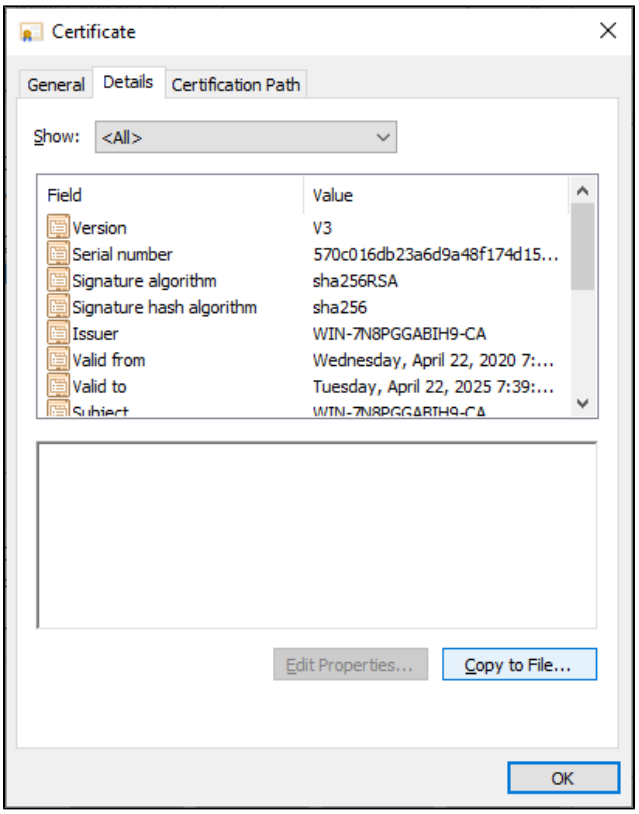
Приступим к настройке VPN. Для аутентификации с помощью сертификатов, необходимо в первую очередь получить корневой сертификат УЦ и запросить у него сертификат для себя. Получить сертификат УЦ можно через менеджер управления УЦ. Кликнем правой кнопкой мыши по нашему УЦ и выберем вкладку "Properties":



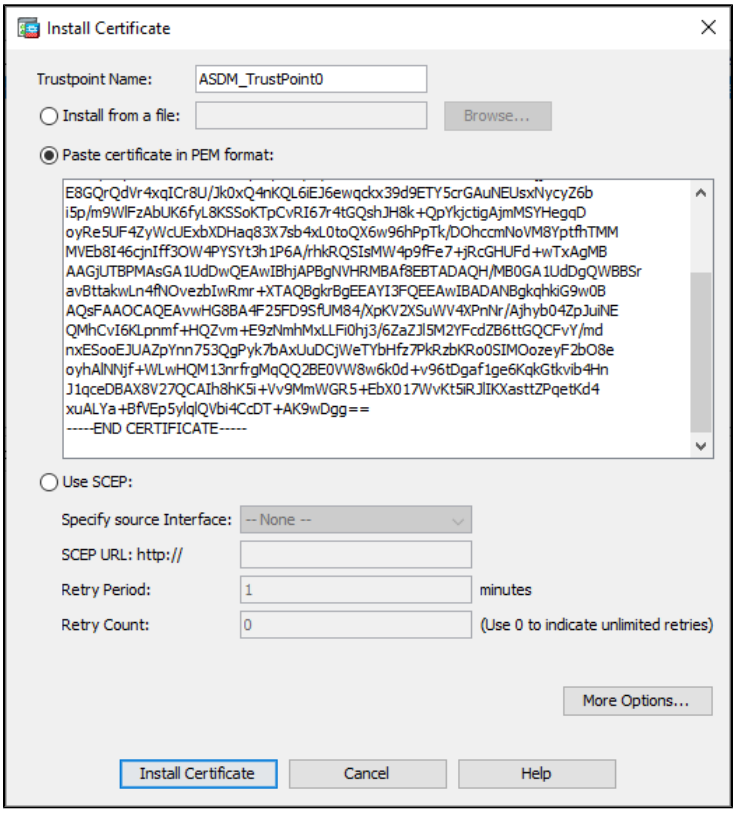
Находим наш корневой сертификат и нажимаем на "View Certificate".



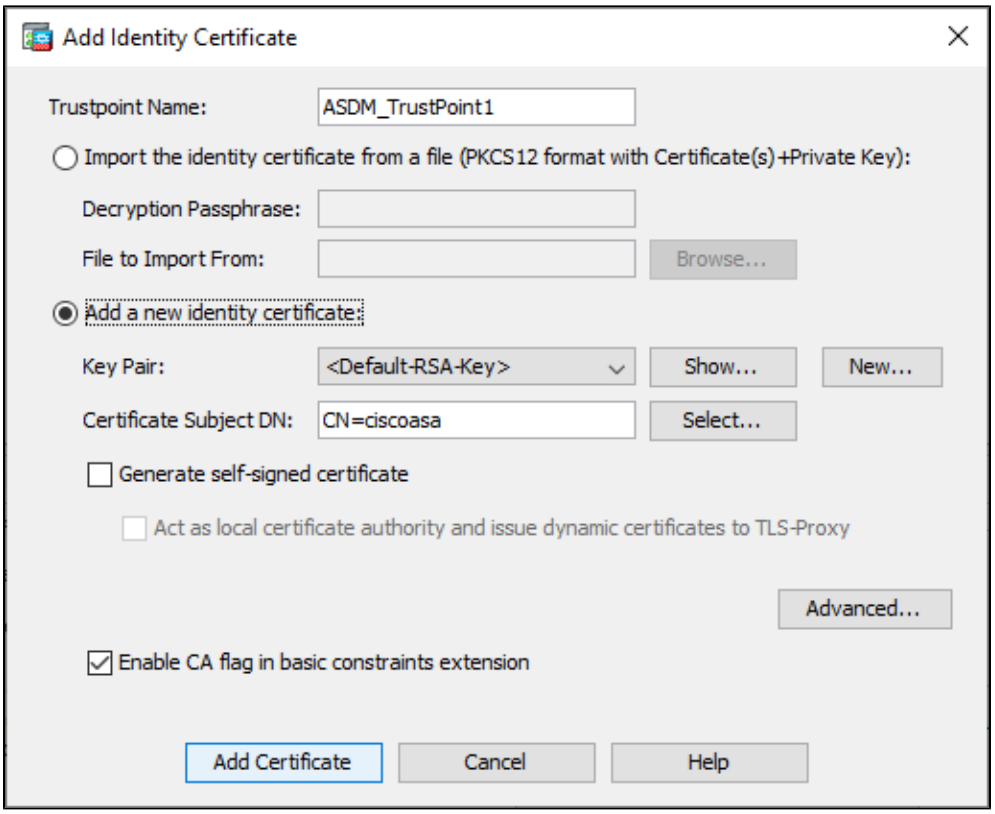
Копируем его в файл в кодировке Base64 и отправляем его в ASDM.



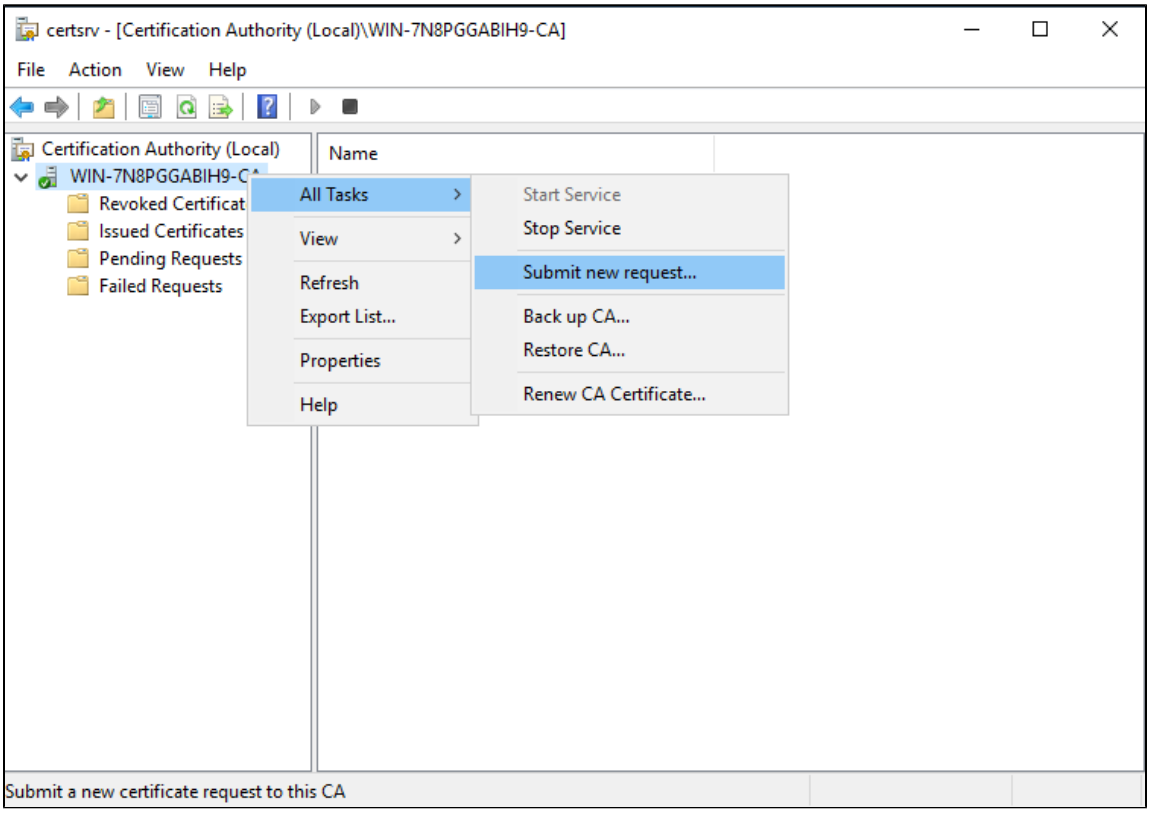
В ASDM выбираем "Configuration"→"Device Management"→"Certificate Management"→"CA Certificates"→"Add" и вставляем туда корневой сертификат УЦ. Я это сделал скопировав содержимое файла сертификата в PEM формате, но можно импортировать его и через файл.



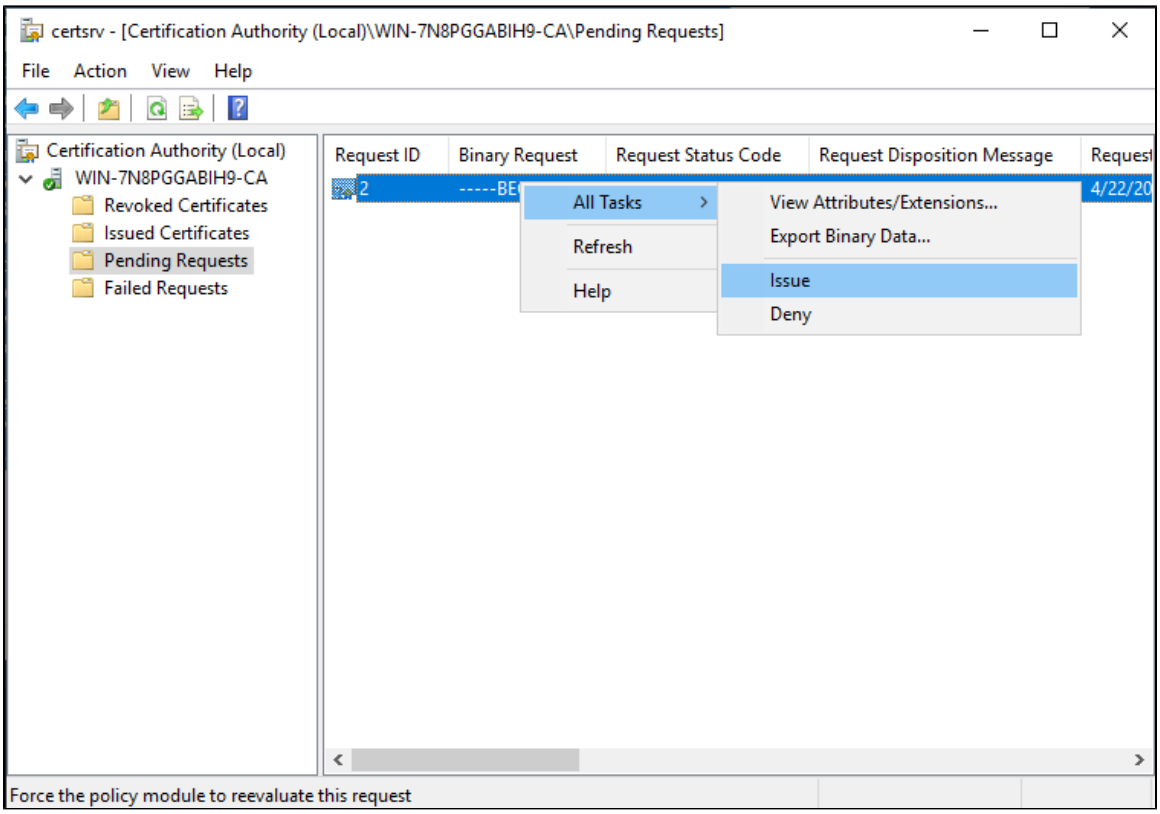
После того как корневой сертификат был импортирован, необходимо создать заявку на сертификат для ASA. Для этого переходим на вкладку "Configuration"→"Device Management"→"Certificate Management"→"Identity Certificates"→"Add" и создаем заявку для ключа по умолчанию:



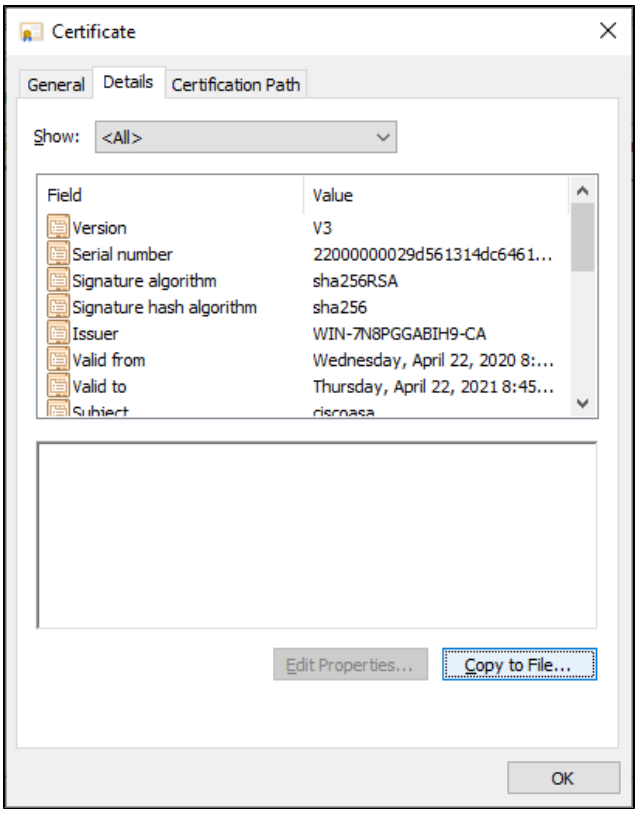
Заявку отправляем на сервер и добавляем ее в менеджер УЦ, кликнув правой кнопкой мыши на сервер и выбрав "All Tasks"→"Submit new request...":



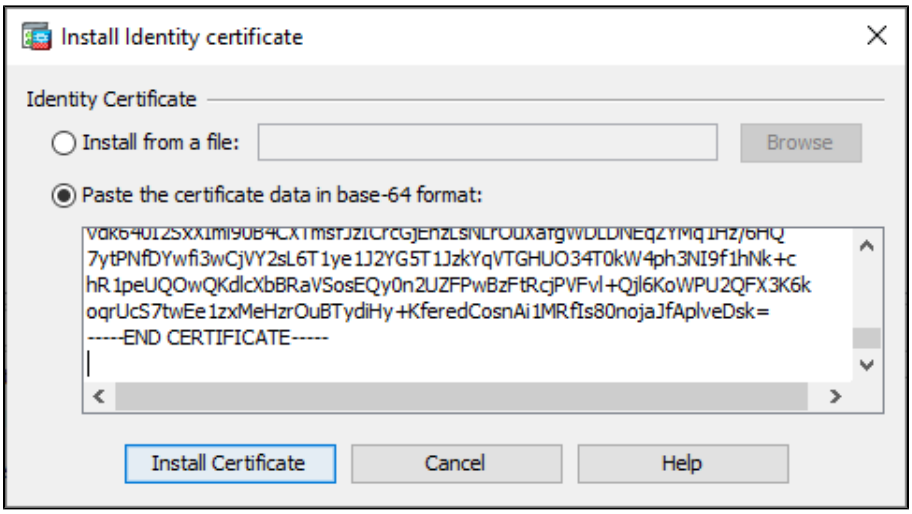
В открывшемся окне указываем путь до заявки и дальше переходим в директорию "Pending requests" и подписываем заявку. Для этого кликнем правой кнопкой мыши на нашей заявке и выбираем "All Tasks"→"Issue":



Подписанный сертификат можно получить в директории "Issued Certificates". Ищем наш сертификат и копируем его в файл в кодировке Base64:

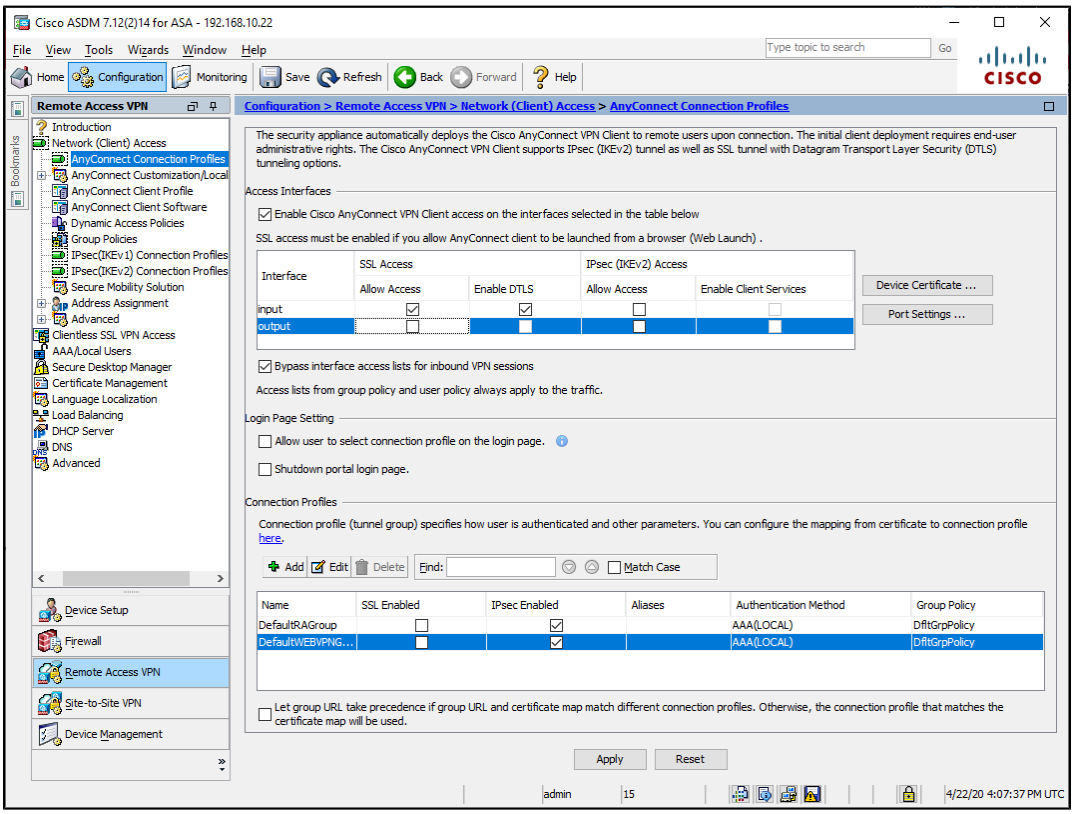


Полученный сертификат отправляем на сторону ASDM и добавляем его на вкладке "Configuration"→"Device Management"→"Certificate Management"→"Identity Certificates"→"Install" для нашего запроса:

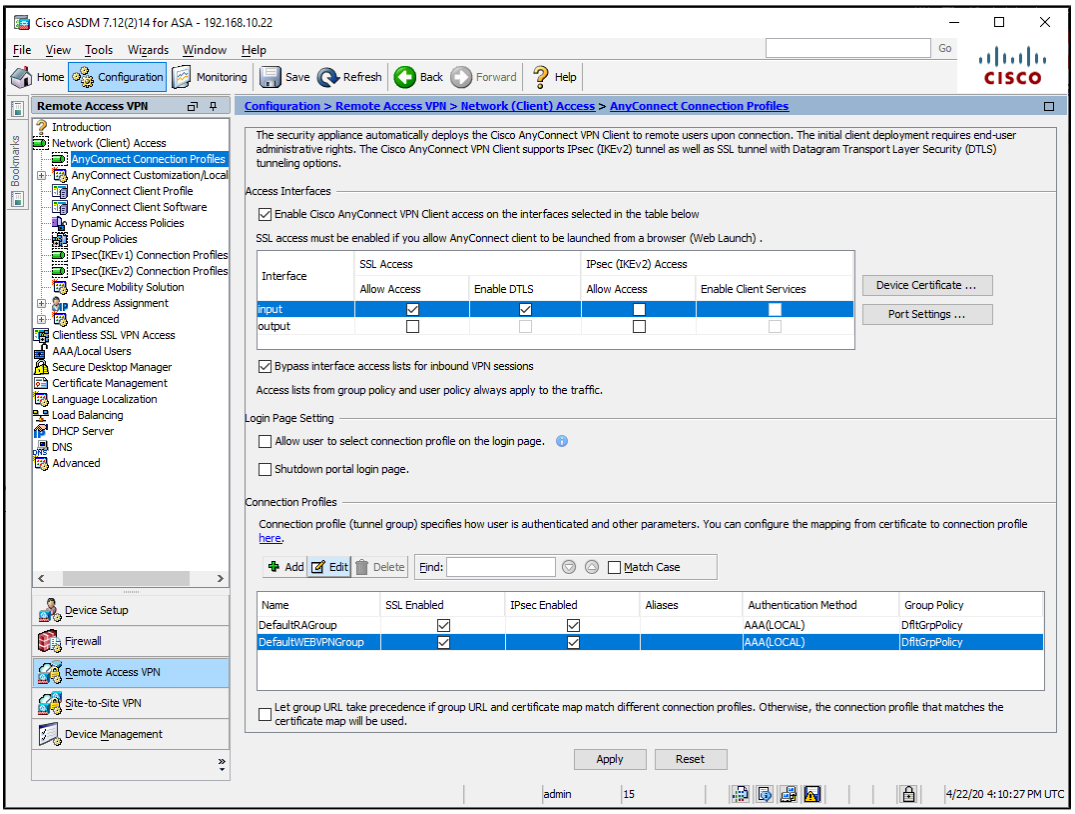


Настройка VPN на ASA

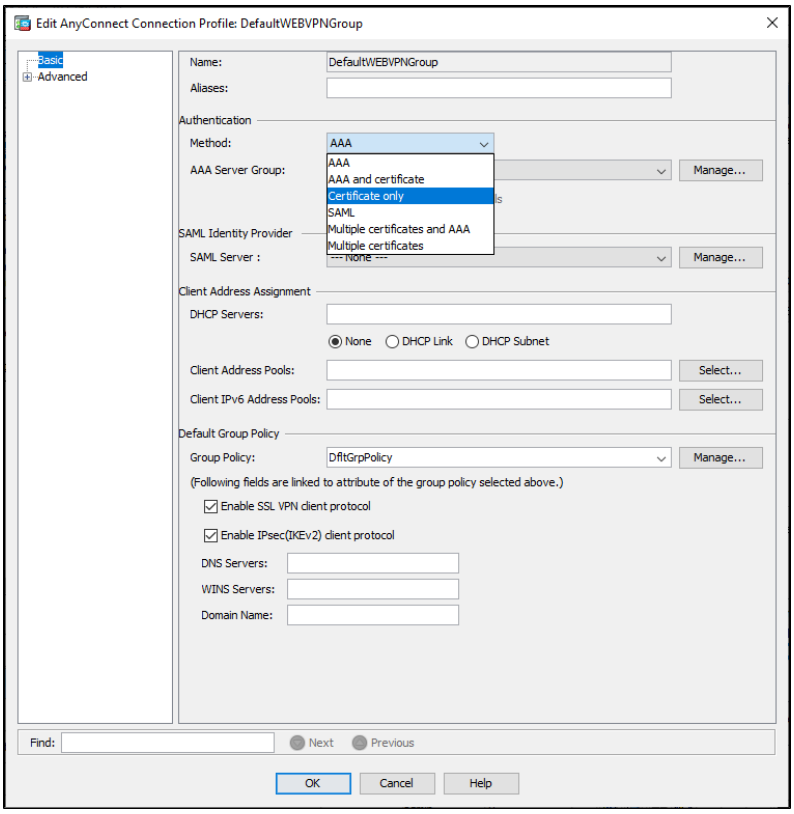
На стороне МЭ осталось настроить сам VPN. Для этого переходим на вкладку "Configuration"→"Remote access VPN"→"Network client Access"→" AnyConnect Connection Profiles". Установим галку напротив "Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below" (после установки данной опции от вас могут потребовать установить в МЭ пакеты с AnyConnect для Windows и Linux). Также необходимо разрешить подключение через входной интерфейс:



Для профиля "DefaultWEBVPNGroup" установим опцию SSL Enabled и отредактируем его, нажав "Edit":

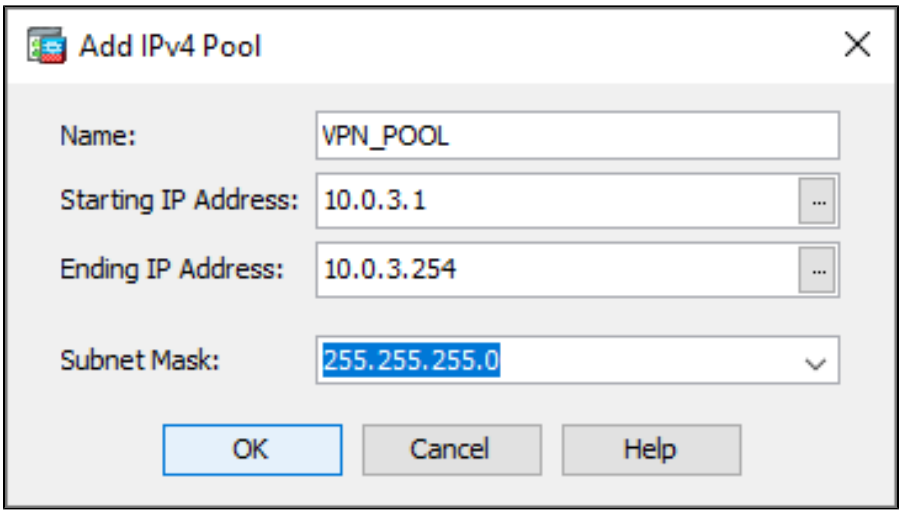


В открывшемся окне установим аутентификацию с помощью сертификата:



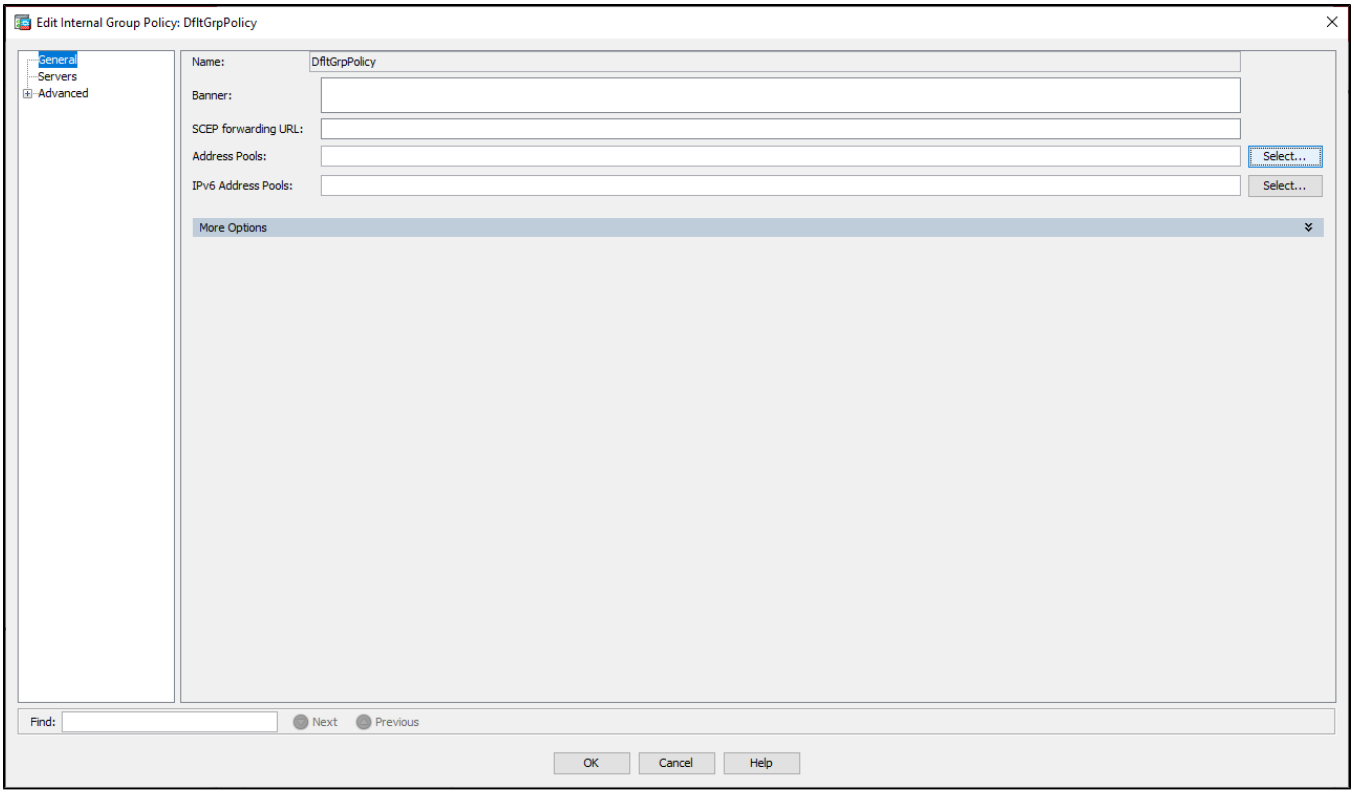
Применим изменения, нажав "Apply".

Теперь необходимо задать диапазон VPN адресов для клиентов. Для этого переходим на вкладку "Configuration"→"Remote access VPN"→" Network client Access"→"Address Assignment"→"Address Pools"→"Add" и создадим свой диапазон:

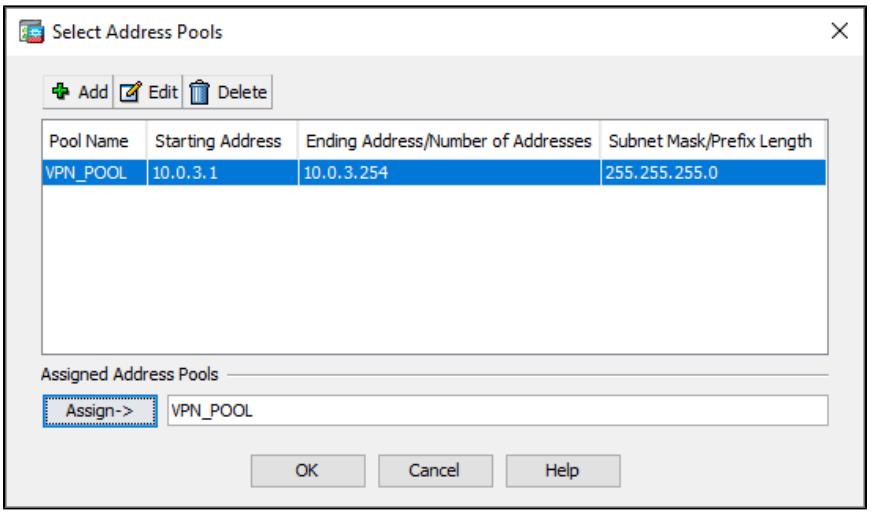


Применяем изменения.

Далее переходим на вкладку "Configuration"→"Remote access VPN"→"Network client Access"→"Group Policy" и дважды кликаем на политику DfltGrpPolicy:



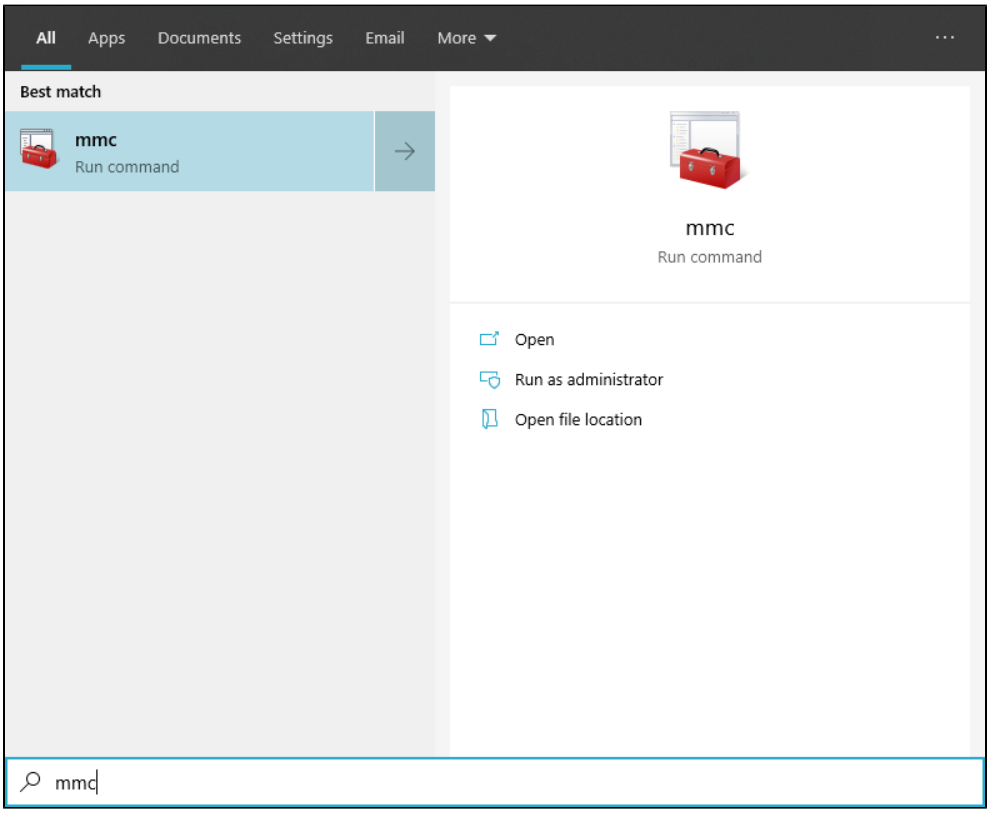
В открывшемся окне устанавливаем выбранный диапазон адресов на вкладке "Address Pools":



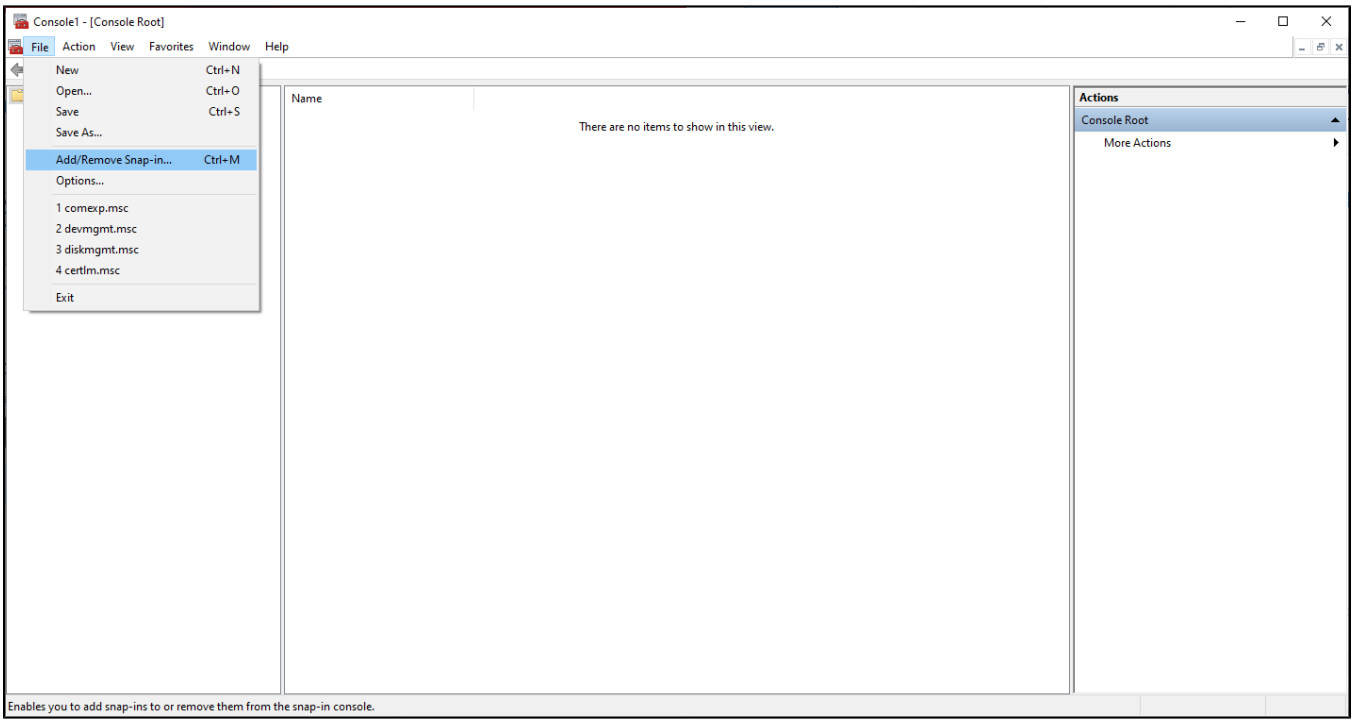
Применяем изменения и нажимаем на кнопку "Save" в панели инструментов.

Настройка клиента VPN в Windows (AnyConnect)

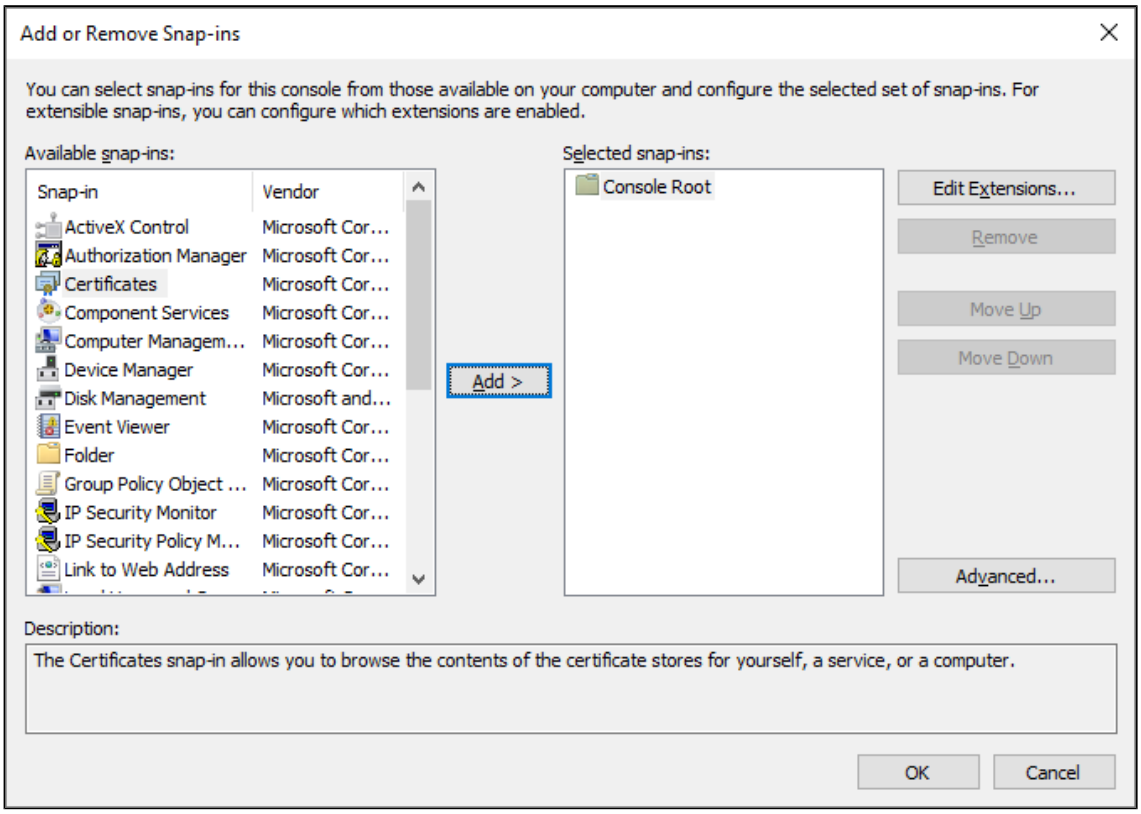
Теперь осталось лишь установить корневой сертификат УЦ на клиенте и получить сертификат у него. Корневой сертификат мы уже с вами получали выше. Для его установки на клиент запустим приложение mmc.



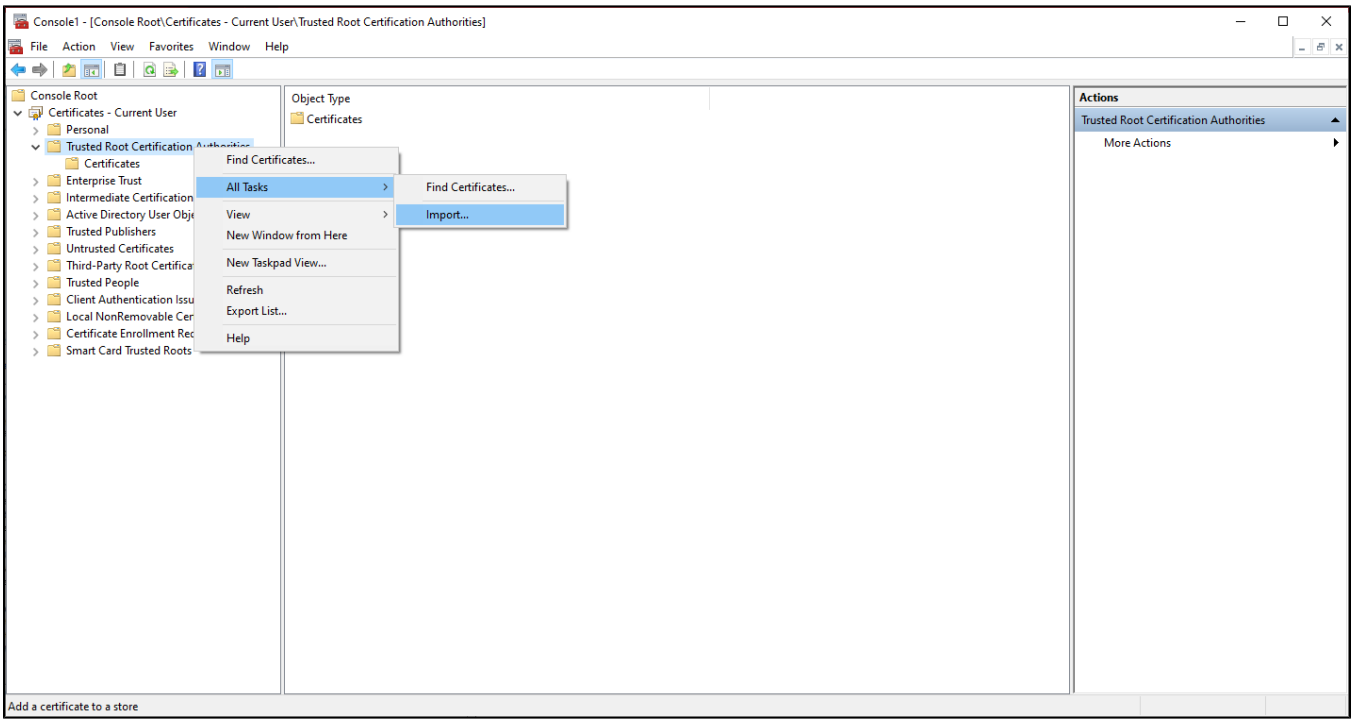
В открывшемся окне выбираем "File"→"Add/Remove Snap-In...".



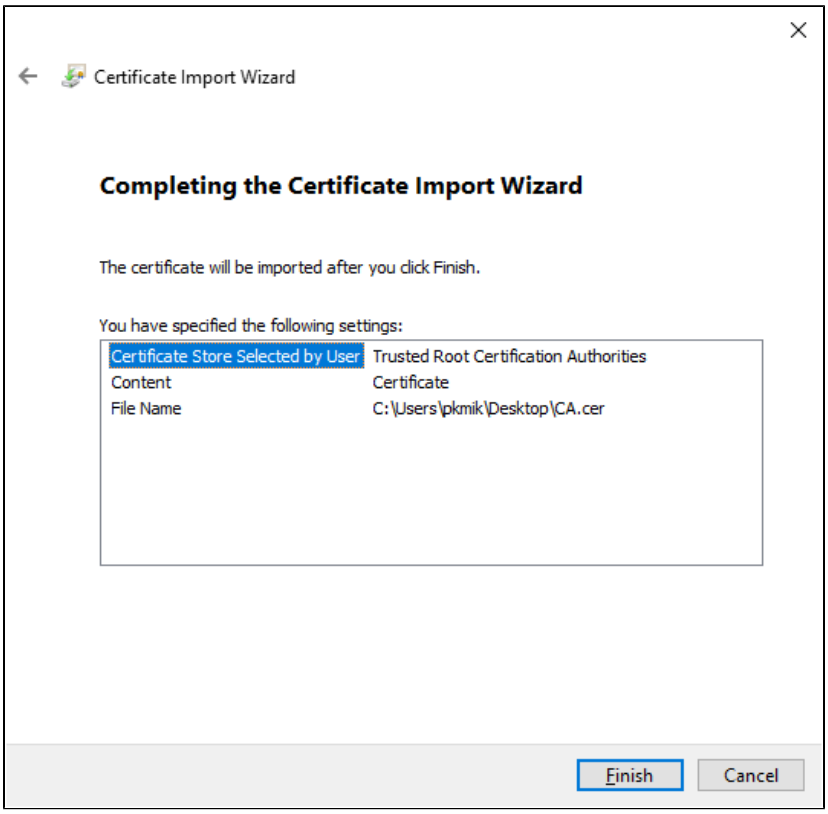
В открывшемся окне выбираем "Certificates" и нажимаем "Add".



Отобразится диалог и в нем необходимо выбрать "My user account". Нажимаем "Ok". В появившемся каталоге необходимо найти каталог "Trusted Root Certification Authorities", нажать на него правой кнопкой мыши и выбрать задачу импортирования нового сертификата:

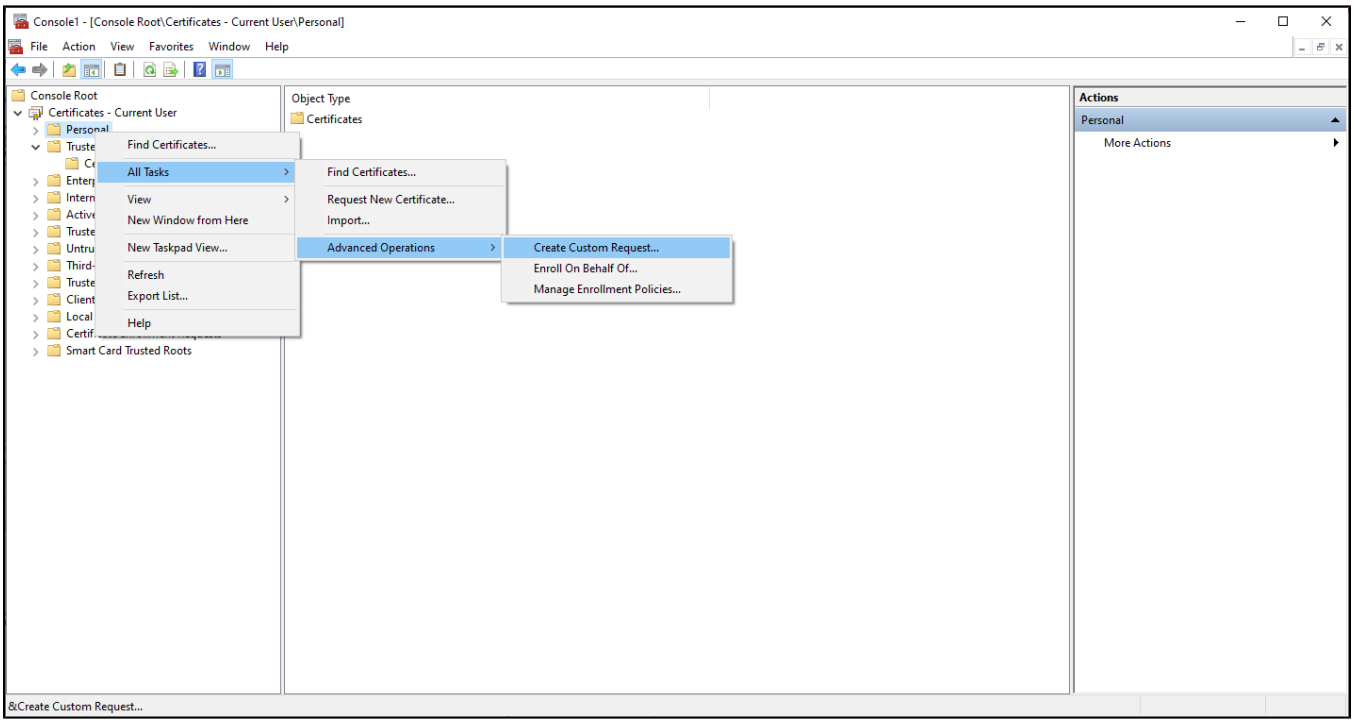


В открывшемся окне указываем путь до корневого сертификата.

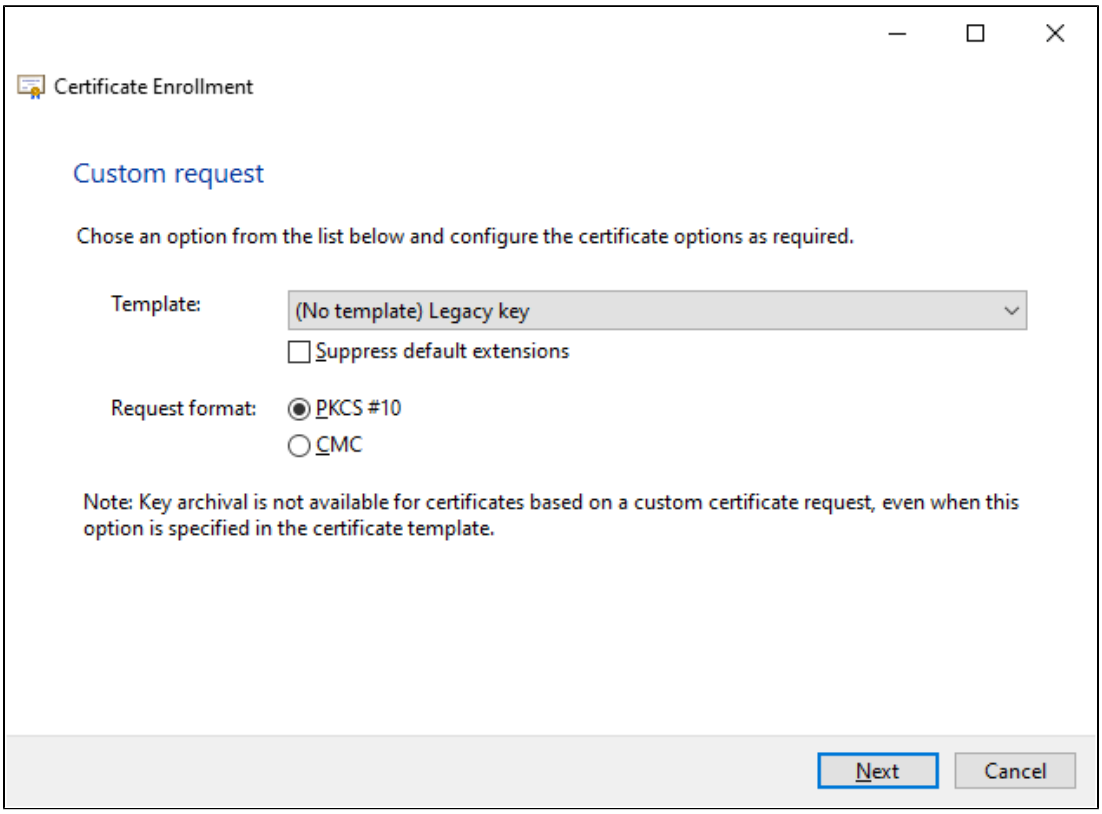


После того как мы импортировали корневой сертификат на наш клиент, необходимо создать заявку на сертификат для ключа, который будет создан на токене. Чтобы в Windows можно было работать с токеном, установим драйверы и подключим токен.

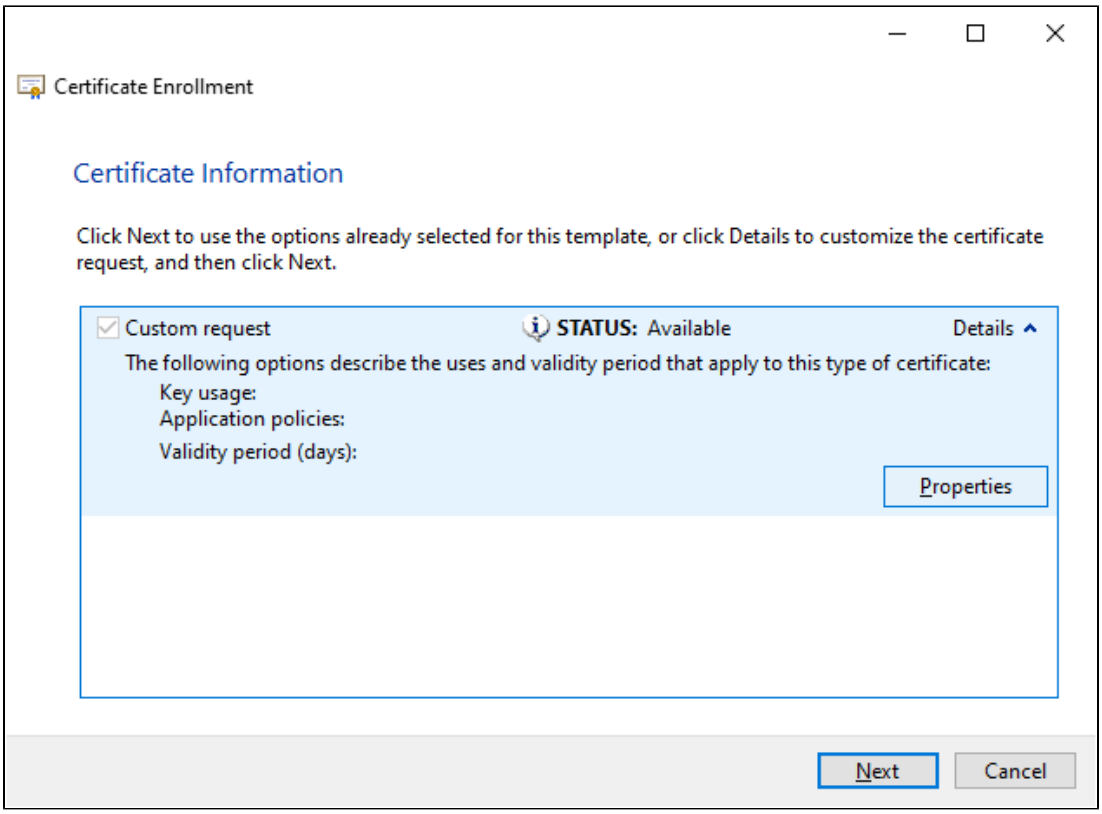
После того как все необходимые действия были выполнены перейдем обратно в mcc и правой кнопкой мыши кликнем по директории "Personal" и выберем задачу создания запроса на сертификат:



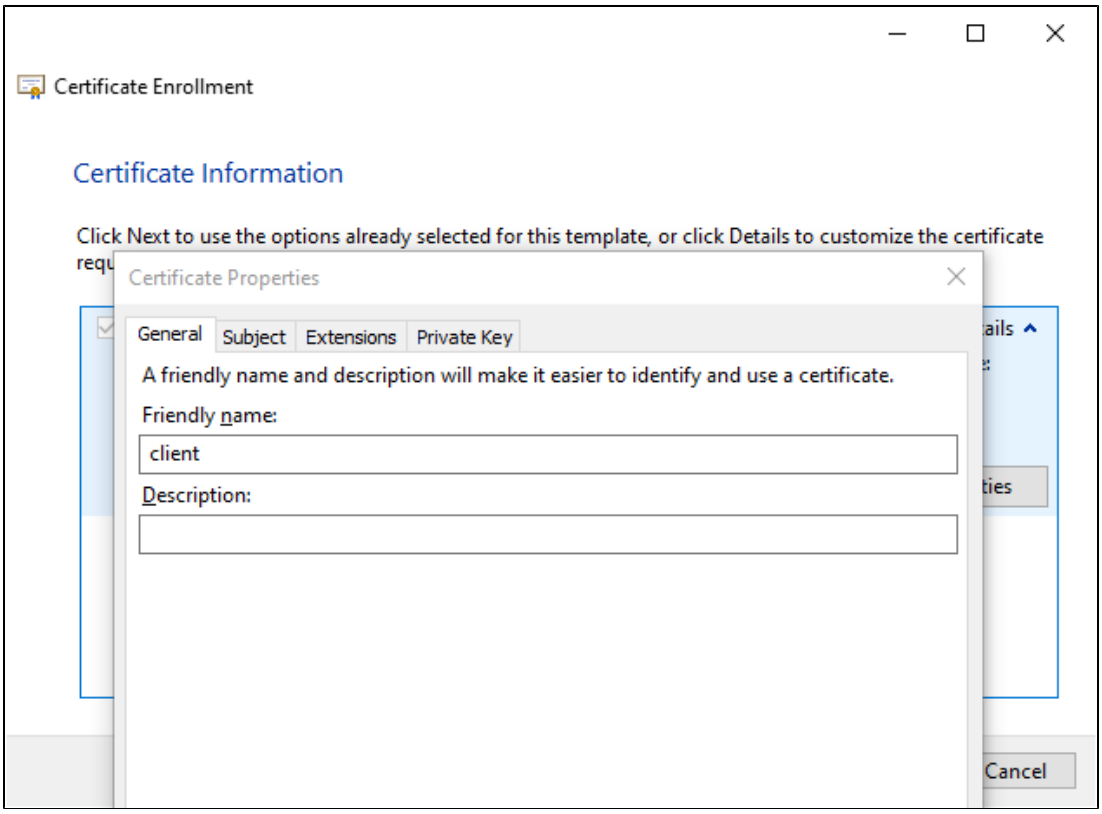
На первых двух вкладках нажимаем "Next" , на третьей выбираем "Legacy key".



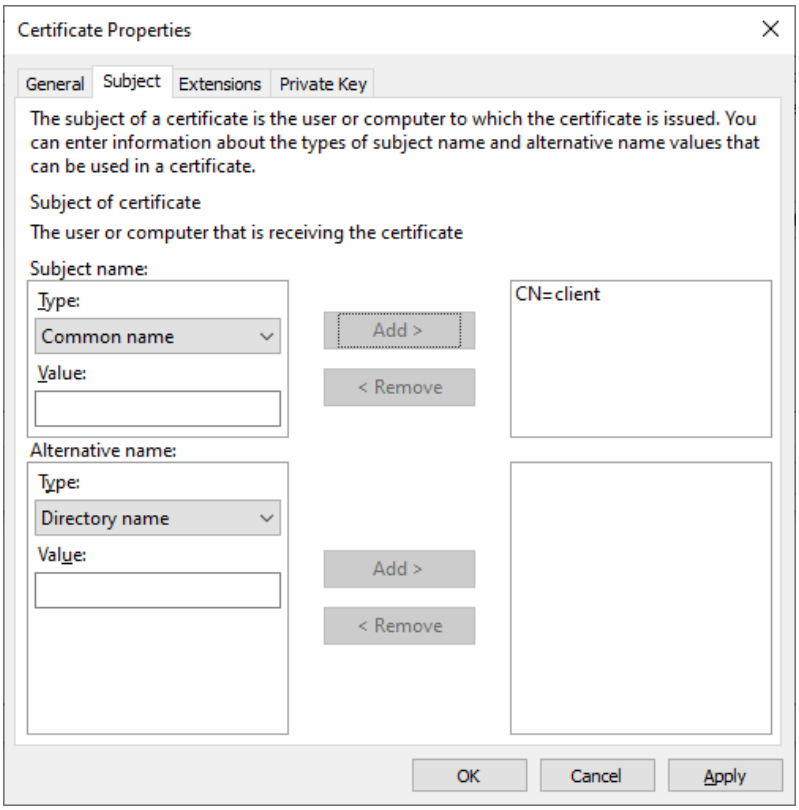
В следующем окне задаем опции заявки и ключа, для которого она будет создана:



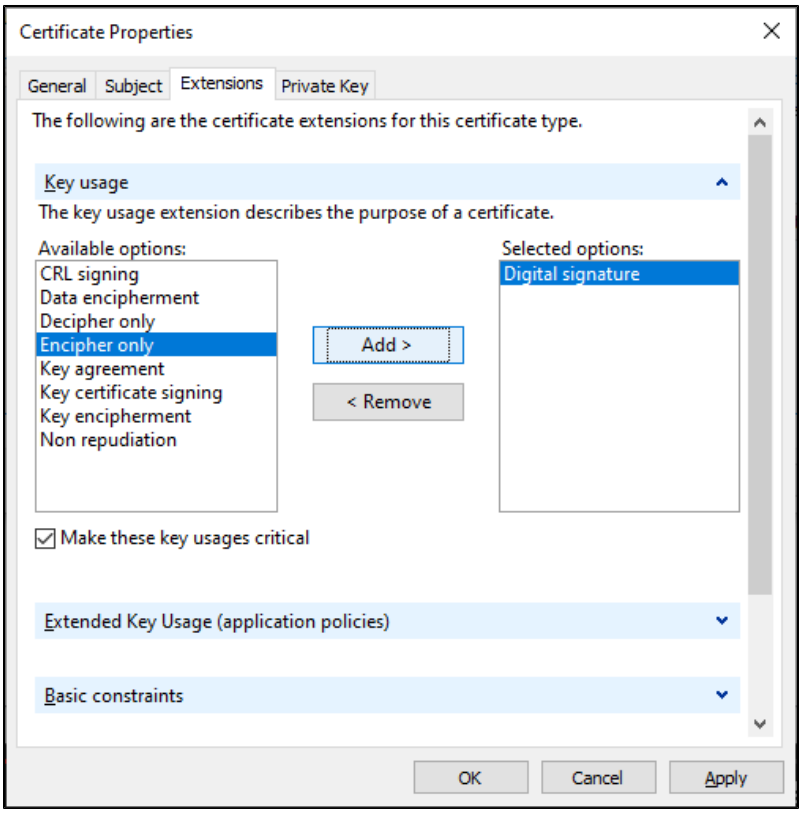
Как минимум: зададим Friendly name – его можно выбрать произвольным, это будет идентификатором вашего пользователя:



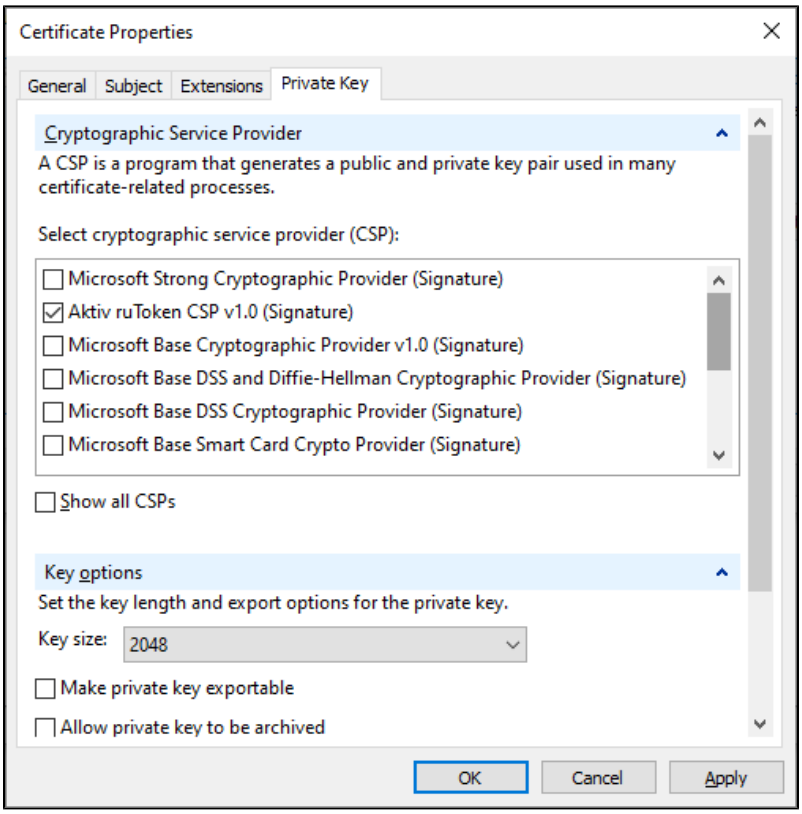
Зададим "Общее имя", оно должно быть идентификатором вашего пользователя:



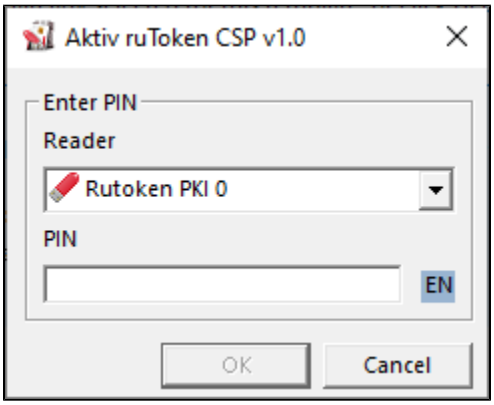
Установим предназначение ключа для подписи:



И для создания ключа на токене укажем криптопровайдер Рутокен и зададим размер ключа в 2048.

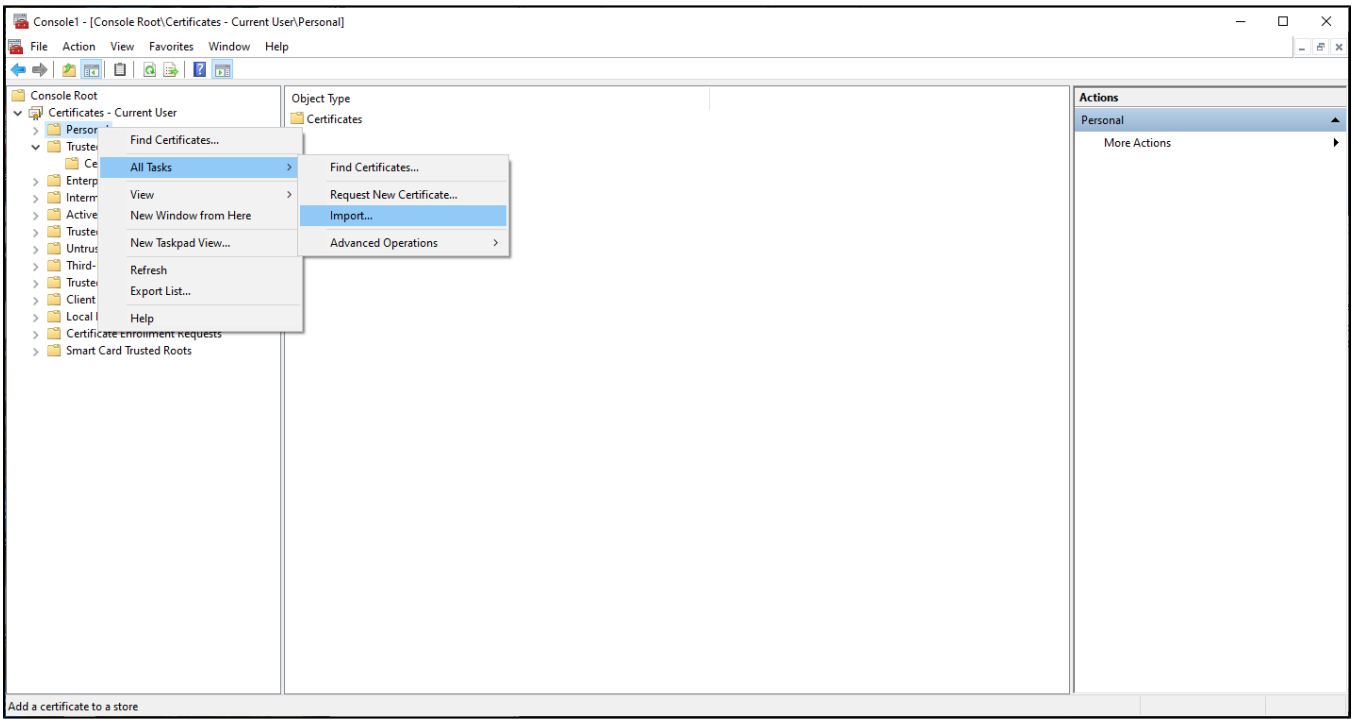


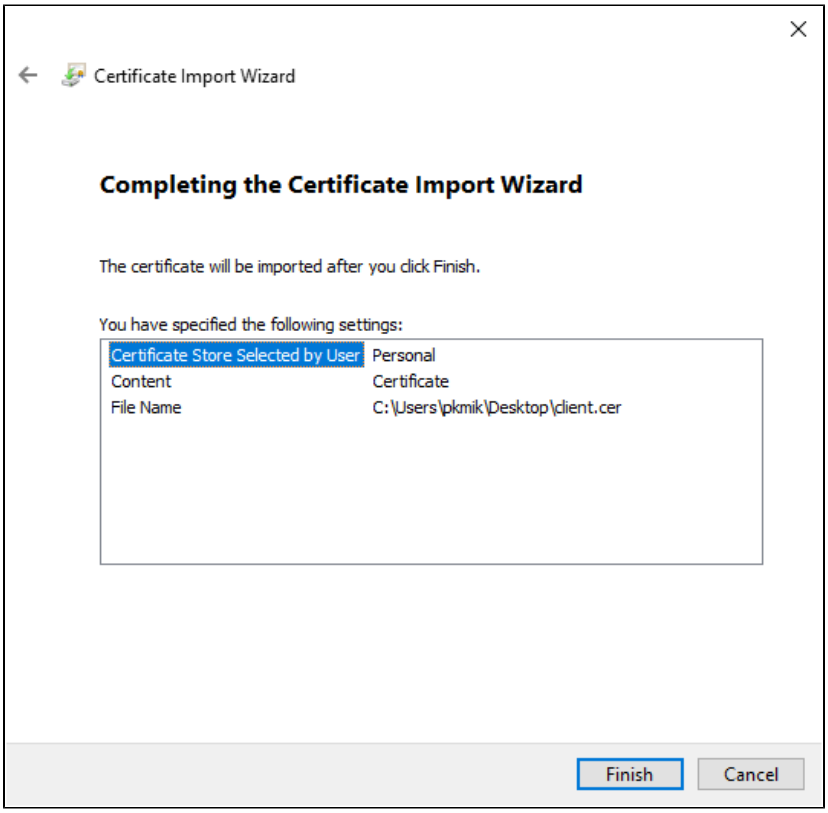
От нас потребуют ввести PIN-код токена:



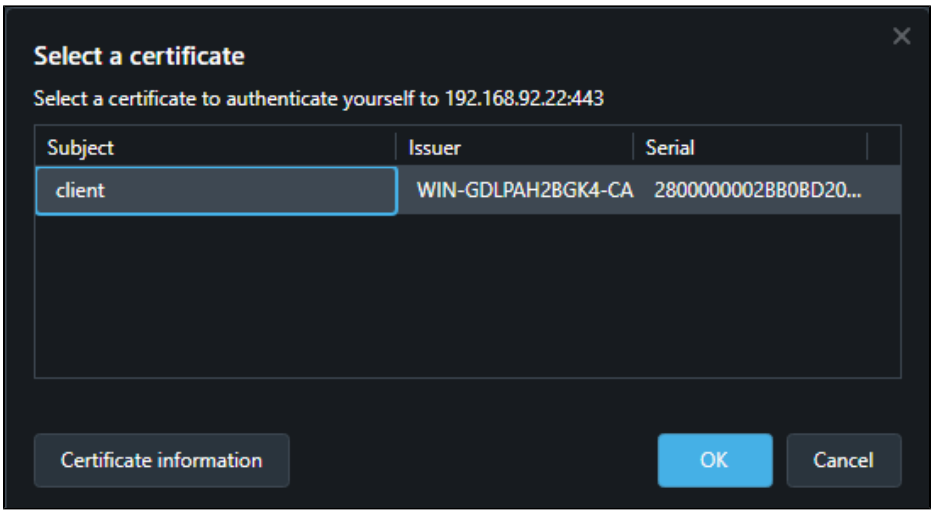
Заявку на сертификат сохраним в файл в кодировке Base64 и отправим ее на сторону УЦ. В УЦ подписываем заявку также как и заявку для ASA из инструкции выше.

Выписанный сертификат импортируем в директорию "Personal" на клиенте:

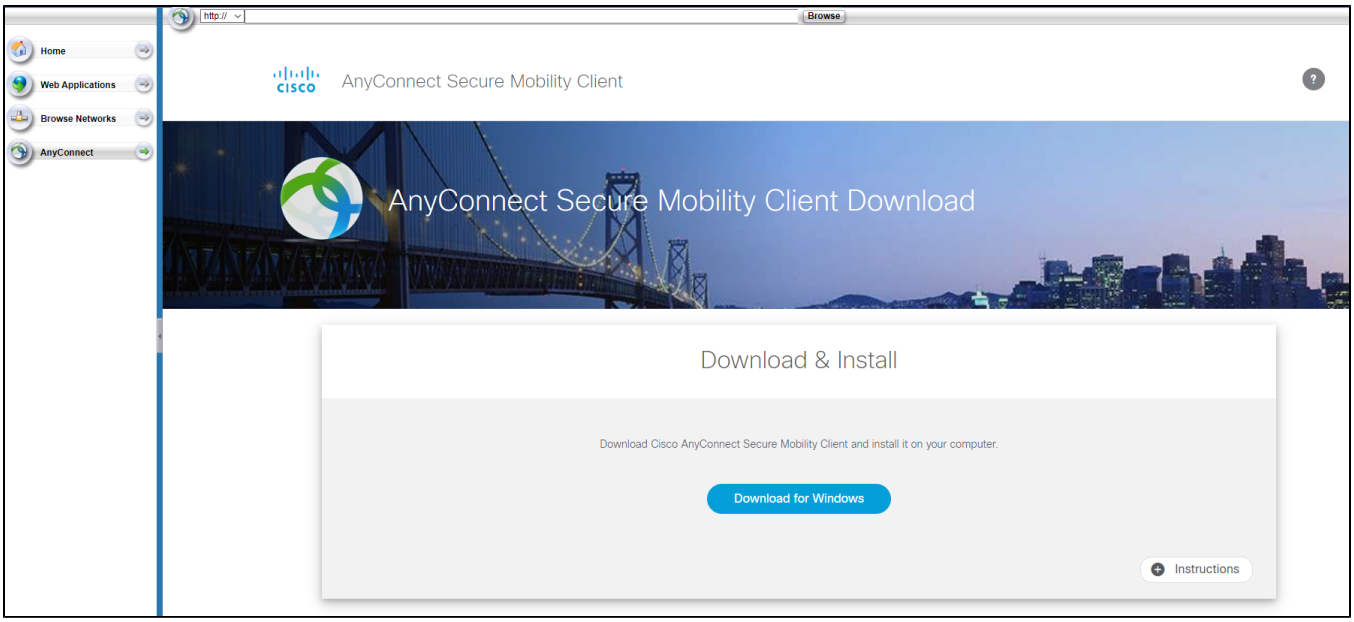




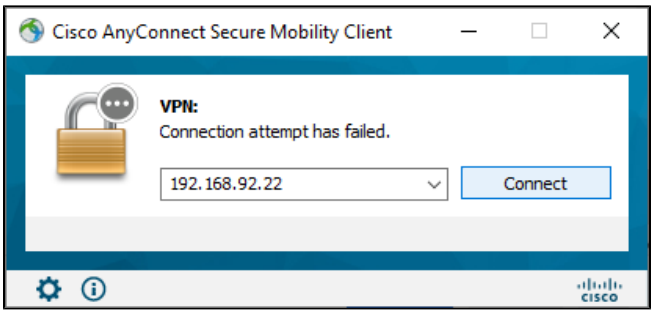
Теперь откроем браузер и подключимся к входному интерфейсу ASA -- https://192.168.92.22. От нас потребует выбрать сертификат, который мы хотим использовать для входа:



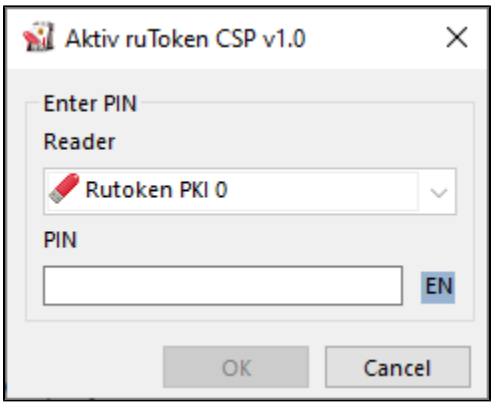
После выбора, будет произведен вход и мы можем скачать anyconnect с открывшейся страницы.



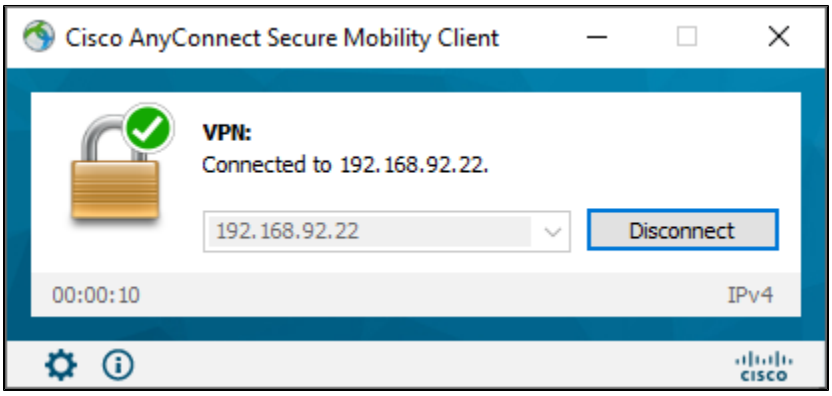
Устанавливаем приложение Cisco AnyConnect и подключаемся к нашему сетевому экрану через интерфейс input. То есть по адресу 192.168.92.22:



В процессе подключение, от нас потребуют ввести PIN-код токена:



Если соединение было установлено, то все шаги были произведены верно:



Настройка клиента VPN в Linux (OpenConnect)

В первую очередь установим все необходимое программное обеспечение. Для этого загрузим библиотеку PKCS#11 для Rutoken отсюда и установим недостающие пакеты:

Установка пакетов

```
sudo apt-get update
sudo apt-get install opensc openconnect libengine-pkcs11-openssl gnutls-bin
```

Сгенерируем новую ключевую пару на токене и заявку на сертификат для нее:

Примечание

Если вы используете OpenSSL 3.0, то необходимо выполнить следующую инструкцию

генерация ключа и заявки на сертификат

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so --id 42 --keypairgen --key-type rsa:2048 -l
openssl
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib/x86_64-linux-gnu/engines-1.1/libpkcs11.so -pre ID:pkcs11 -pre
LIST_ADD:1 -pre LOAD -pre MODULE_PATH:/usr/lib/librtpkcs11ecp.so
OpenSSL> req -engine pkcs11 -new -key 0:42 -keyform engine -out client.req -outform PEM -subj "/CN=client2"
```

Импортируем полученную заявку на токен:

импорт сертификата на токен

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y cert -w client.cer --id 42
```

Настроим p11tool, чтобы он мог видеть Рутокен и проверим, что токен распознается.

Настройка p11tool

```
sudo sh -c "echo 'module:/usr/lib/librtpkcs11ecp.so' > /usr/share/p11-kit/modules/opensc.module"
p11tool --list-tokens
```

Вывод должен быть таким:

```
lo1ol@lo1ol-virtual-machine:~/Downloads$ p11tool --list-tokens
Token 0:
        URL: pkcs11:model=p11-kit-trust;manufacturer=PKCS%2311%20Kit;serial=1;t
oken=System%20Trust
        Label: System Trust
        Type: Trust module
        Manufacturer: PKCS#11 Kit
        Model: p11-kit-trust
        Serial: 1
        Module: p11-kit-trust.so


Token 1:
        URL: pkcs11:model=Rutoken%20ECP;manufacturer=Aktiv%20Co.;serial=363441c
a;token=Rutoken%20ECP%20%3cno%20label%3e
        Label: Rutoken ECP <no label>
        Type: Hardware token
        Manufacturer: Aktiv Co.
        Model: Rutoken ECP
        Serial: 363441ca
        Module: /usr/lib/librtpkcs11ecp.so
```

Запоминаем URL Рутокена и узнаем путь до сертификатов на нем:

Узнаем пути до сертификатов на токене

```
p11tool –list-all-certs "pkcs11:model=Rutoken%20ECP;manufacturer=Aktiv%20Co.;serial=363441ca;token=Rutoken%
20ECP%20%3cno%20label%3e"
```

Вывод должен быть таким:

```
lo1ol@lo1ol-virtual-machine:~/Downloads$ p11tool --list-all-certs "pkcs11:model
=Rutoken%20ECP;manufacturer=Aktiv%20Co.;serial=363441ca;token=Rutoken%20ECP%20%
3cno%20label%3e"
Object 0:
        URL: pkcs11:model=Rutoken%20ECP;manufacturer=Aktiv%20Co.;serial=363441c
a;token=Rutoken%20ECP%20%3cno%20label%3e;id=%42;type=cert
        Type: X.509 Certificate
        Label:
        ID: 42
```

Данный URL нужно использовать, чтобы указать путь для сертификата для OpenConnect:

Подключение к VPN с использованием сертификата на токене

```
sudo openconnect -c "pkcs11:model=Rutoken%20ECP;manufacturer=Aktiv%20Co.;serial=363441ca;token=Rutoken%20ECP%20%
3cno%20label%3e;id=%42;type=cert" 192.168.92.22
```

Запустите отдельное окно с командной строкой и посмотрите, создался ли интерфейс tun0, если он создался, то настройка прошла успешно:

```
lo1ol@lo1ol-virtual-machine:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 00:0c:29:cd:fa:b3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.135/24 brd 192.168.10.255 scope global dynamic noprefixrout
e ens33
       valid_lft 1603sec preferred_lft 1603sec
    inet6 fe80::c9d3:1861:9402:a877/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1406 qdisc fq_codel stat
e UNKNOWN group default qlen 500
    link/none
    inet 10.0.3.2/32 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::f924:1a20:8c5e:198/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

Настройка закончена.