

Контроллер беспроводной сети NETGEAR ProSAFE WC7520

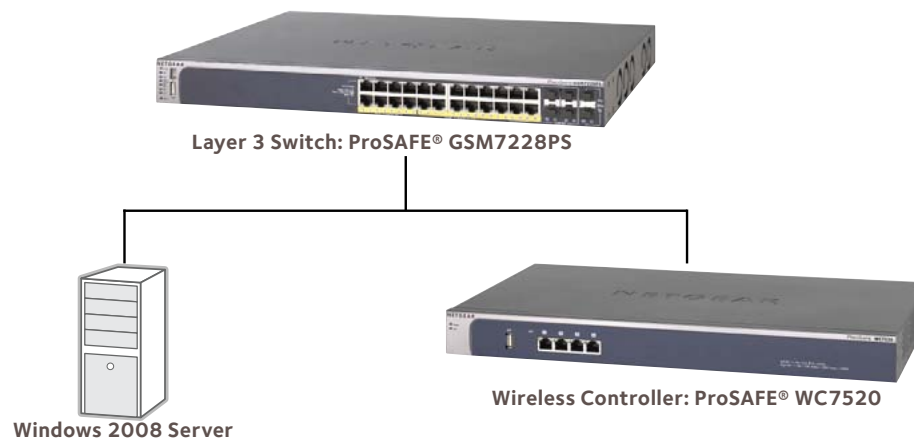
Использование Active Directory для аутентификации
пользователей беспроводной сети

КОРОТКО О ГЛАВНОМ

Доступ к корпоративным сетям требуется широкому спектру групп пользователей с разными потребностями. К этим группам могут применяться различные политики безопасности. Для разделения пользователей важно в первую очередь произвести аутентификацию, выяснить его принадлежность к той или иной группе. Этот документ опишет процесс настройки аутентификации пользователей на контроллере беспроводной сети NETGEAR ProSAFE WC7520 с помощью базы Active Directory.

ОБЗОР РЕШЕНИЯ

Используя контроллер NETGEAR ProSAFE WC7520 можно легко производить аутентификацию пользователей, используя данные Active Directory (AD). В этом документе мы будем использовать Windows 2008R2 в качестве AD сервера. NETGEAR ProSAFE WC7520 и AD сервер располагаются в той же подсети и объединены Layer 3 коммутатором NETGEAR ProSAFE GSM7228PS.

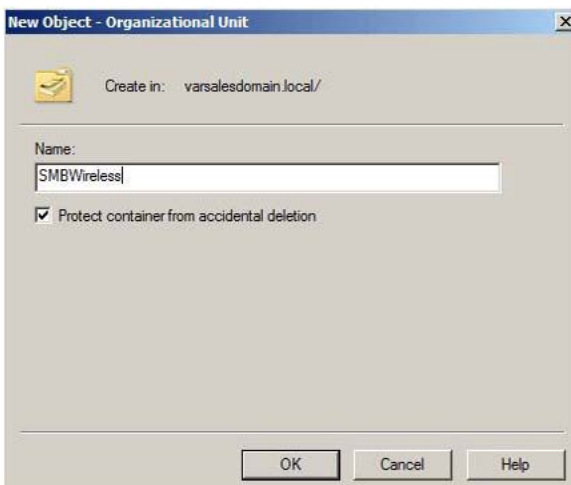
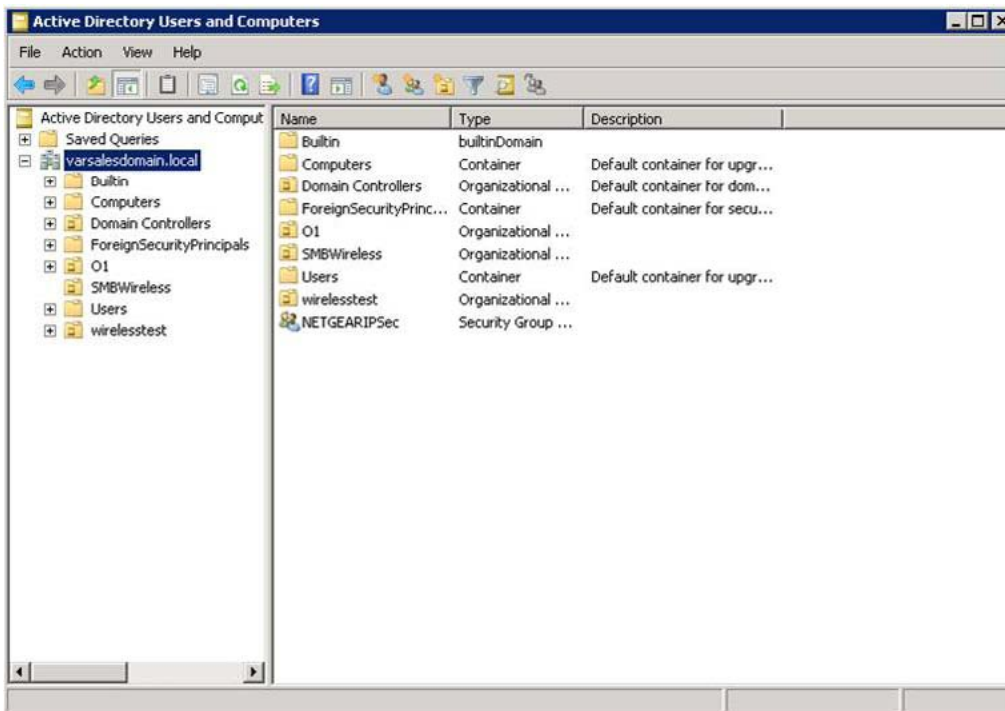


НАСТРОЙКА

Active Directory

Шаг 1 – создание Organizational Unit (OU) для пользователей беспроводной сети

Создайте OU для пользователей беспроводной сети с помощью оснастки *Active Directory Users and Computers*. В этом примере мы будем использовать OU SMBWireless.



Шаг 2 – создание нового пользователя

Создадим в OU SMBWireless нового пользователя. Например, мы создадим нового пользователя *Test*.

The screenshot shows the 'New Object - User' dialog box with the following fields and values:

- Create in: varsalesdomain.local/SMBWireless
- First name: Test
- Initials: (empty)
- Last name: (empty)
- Full name: Test
- User logon name: Test @varsalesdomain.local
- User logon name (pre-Windows 2000): VARSALESDOMAIN\, Test

Buttons: < Back, Next >, Cancel

The screenshot shows the 'New Object - User' dialog box with the following fields and options:

- Password: (masked with dots)
- Confirm password: (masked with dots)
- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

Buttons: < Back, Next >, Cancel

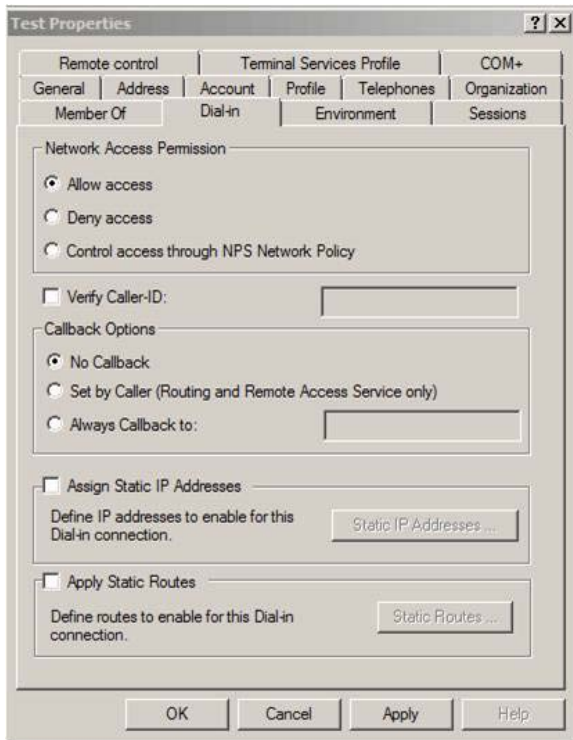
The screenshot shows the 'New Object - User' dialog box with the following summary information:

- When you click Finish, the following object will be created:
- Full name: Test
- User logon name: Test@varsalesdomain.local
- The user cannot change the password.
- The password never expires.

Buttons: < Back, Finish, Cancel

Шаг 3 – откройте доступ новому пользователю

Для этого кликните правой кнопкой мыши на пользователе *Test* и в выпадающем меню выберите *Properties* (Свойства). Убедитесь что в вкладке Dial-IN выбрана опция *Allow Access*.



WC7520

Шаг 1 – настройка IP адреса WC7520 с тем, чтобы он находился в той же подсети, что и сервер AD

Пройдите аутентификацию на WC7520 и выберите пункт меню *Configuration – System – IP/VLAN* чтобы настроить IP адрес WC7520. В данном примере мы будем использовать 192.168.1.125 в качестве AD/DNS сервера, 192.168.1.250 в качестве адреса WC7520.

NETGEAR®
Connect with Innovation™

Access Point | **Configuration** | Monitor | Maintenance | Stacking | Plans | Diagnostics

System | Wireless | Security | Profile | WLAN Network | Captive Portal

- > General
- > Time
- > **IP/VLAN**
- > DHCP Server
- > Certificates
- > Alerts

IP Settings

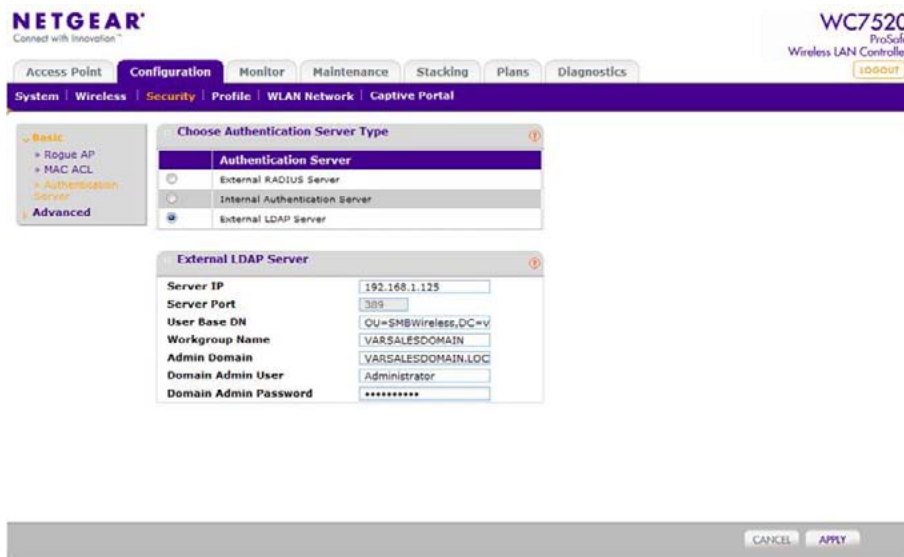
IP Address	192.168.1.250
IP Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary DNS Server	192.168.1.125
Secondary DNS Server	
WINS Server	

Management VLAN Settings

Management VLAN	1
<input checked="" type="checkbox"/> Untagged VLAN	1

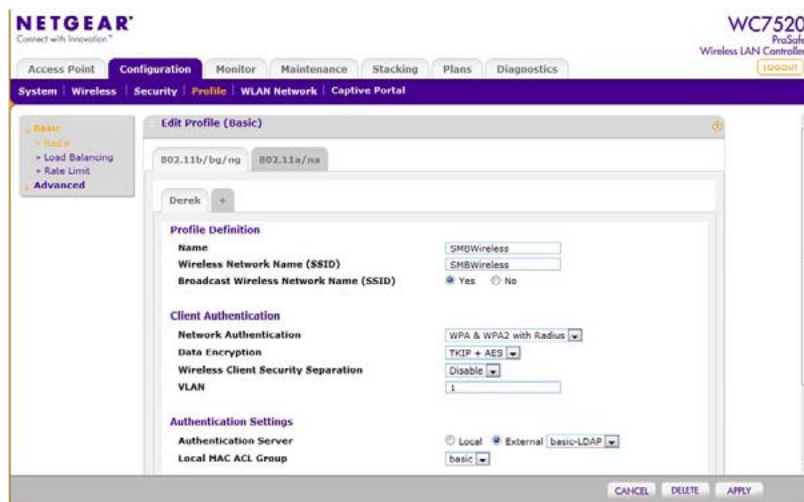
Шаг 2 – настройка точки аутентификации на AD сервере

Выберите пункт меню *Configuration – Security – Authentication Server* и установите радио-точку в *External LDAP Server*. Введите IP адрес AD сервера, User Base DN, учетные данные для аутентификации в Active Directory. В этом примере мы будем использовать адрес AD сервера 192.168.1.125, DN *OU=SMBWireless,DC=varsalesdomain,DC=local* и учетные данные доменного пользователя *Administrator*.



Шаг 3 – настройка SSID

Выберите пункт меню *Configuration – Profile – Basic – Radio* для того, чтобы создать SSID с типом аутентификации WPA & WPA2 with Radius, методом шифрования TKIP + AES и точкой аутентификации установленный в опцию выбора внешнего сервера (External – basic-LDAP).



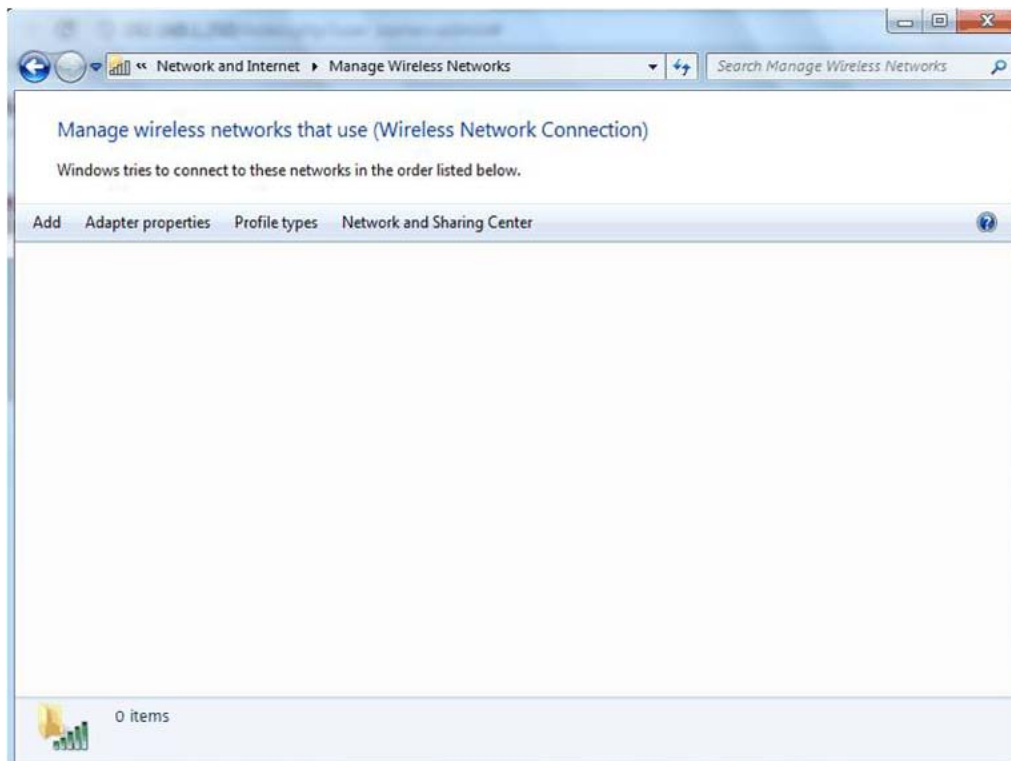
После этой процедуры остается настроить PC для того, чтобы убедиться в способности пользователя проходить аутентификацию в Active Directory.

PC

В этом примере мы будем использовать PC под управлением Windows 7.

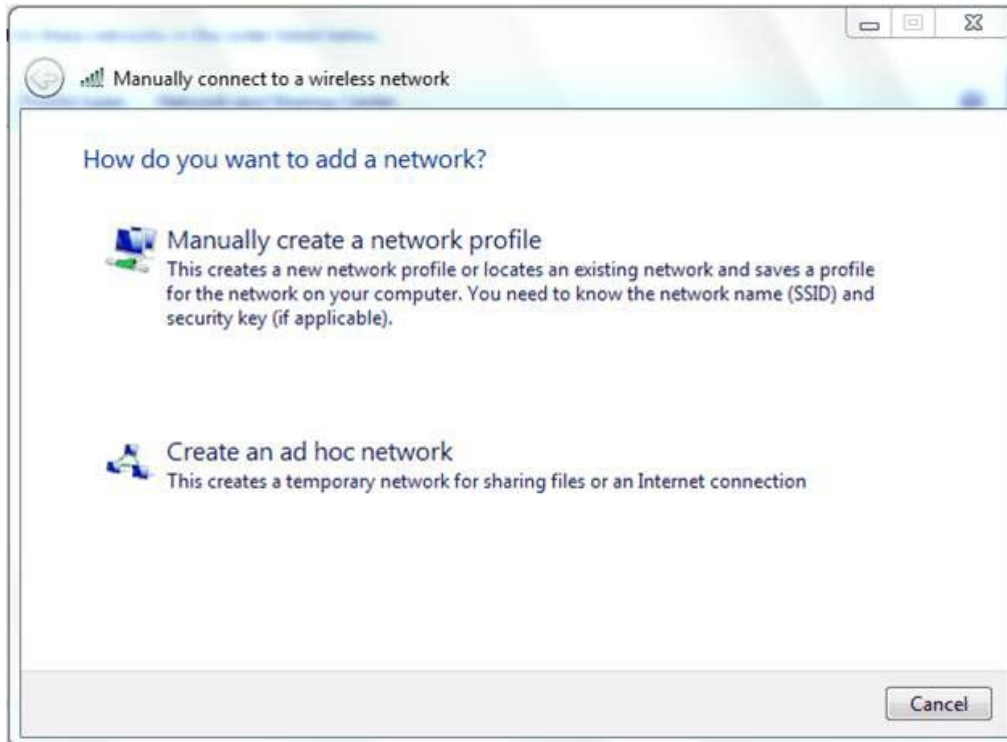
Шаг 1 – добавление беспроводной сети

В панели управления выберите пункт «Network and Internet», а затем «Manage Wireless Networks» с тем, чтобы добавить новую сеть.



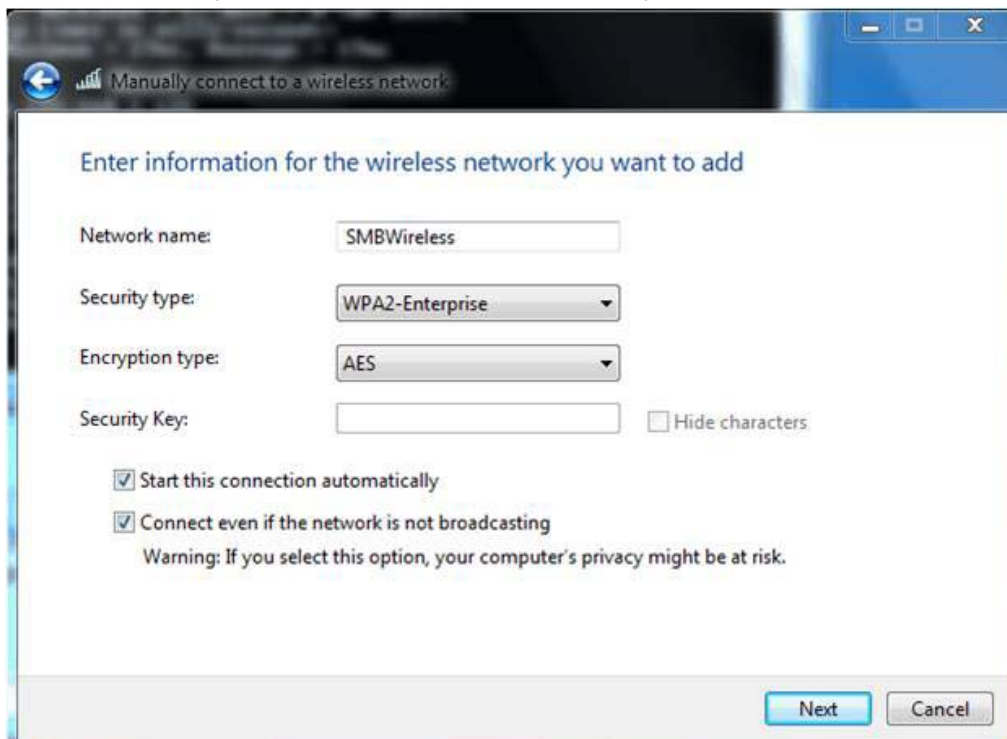
Шаг 2 – создание сетевого профиля

Выберите пункт *Manually create a network profile*.



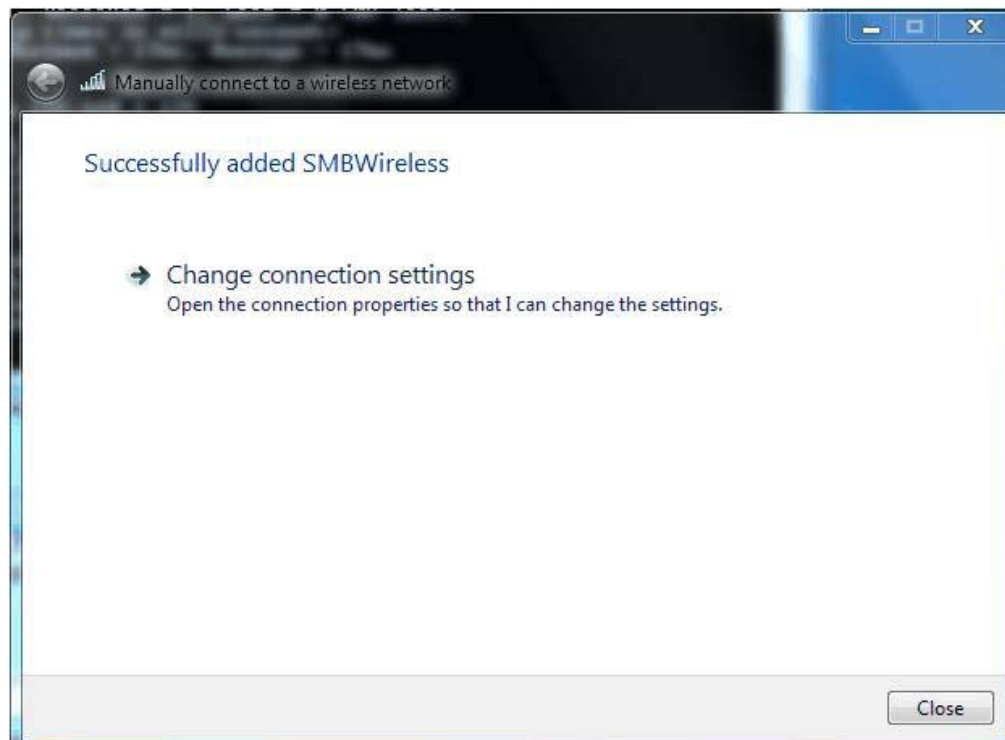
Шаг 3 – настройка SSID

Введите SSID беспроводной сети так, как это было настроено на WC7520 (*SMBWireless*) и нажмите *Next*.



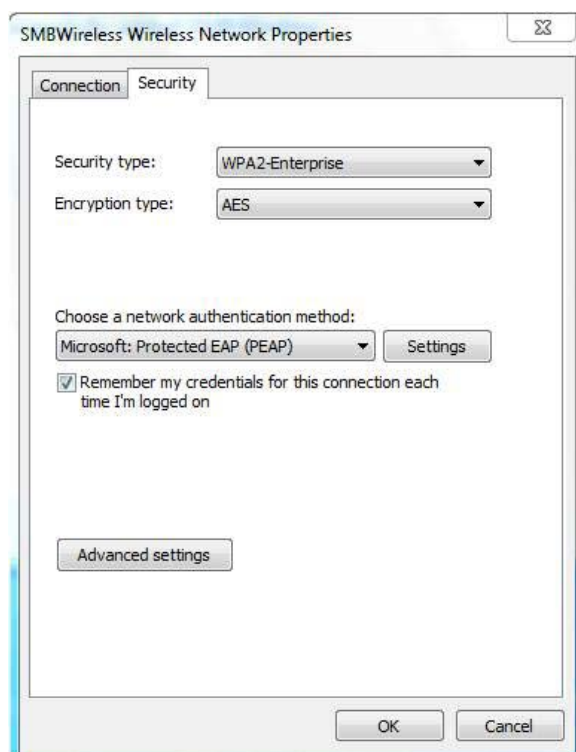
Шаг 4 – настройка беспроводного подключения

Выберите пункт *Change connection settings*.



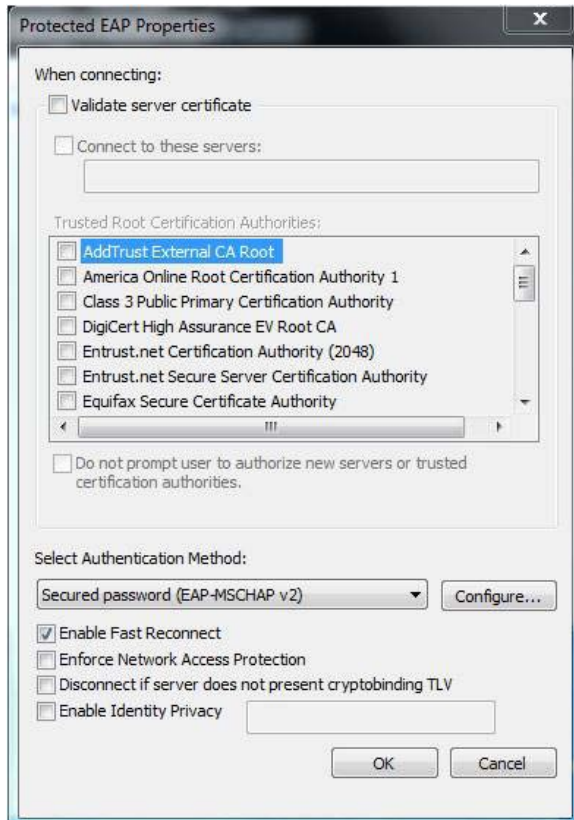
Шаг 5 – изменение настроек безопасности

На вкладке *Security* нажмите на кнопку *Settings* под *Choose a network authentication method*.



Шаг 6 – изменение настроек EAP

Отключите опцию *Validate Server Certificate* и нажмите клавишу *Configure* под *Select Authentication Method*.



Шаг 7 – отключение автоматического использования учетных данных

Отключите автоматическое использование учетных данных, используемых в процессе аутентификации в операционной системе.



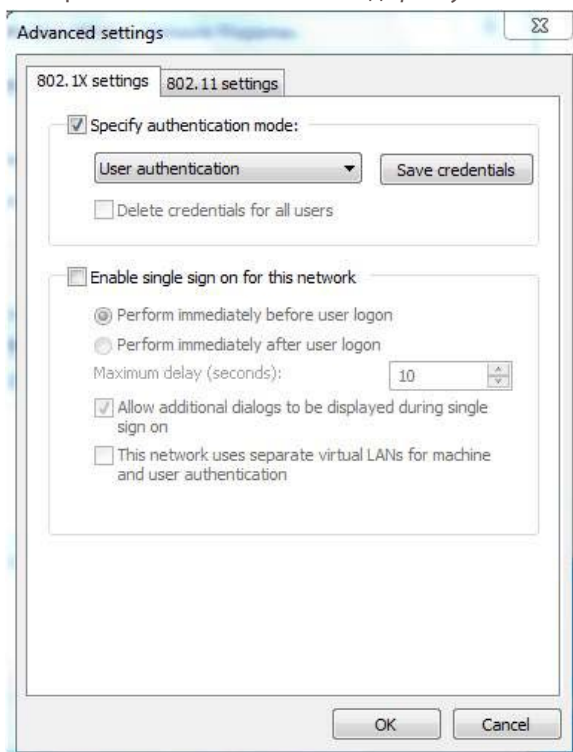
Шаг 8 – изменение настроек безопасности

Нажмите кнопку *Advanced settings*.



Шаг 9 – включение аутентификации пользователей

Выберите *User authentication* под *Specify authentication mode*.



После сохранения этих настроек PC должен подключиться к беспроводной сети. В процессе подключения возникнет диалоговое окно, запрашивающее имя пользователя и пароль. Используйте учетные данные пользователя, созданного в OU SMBWireless. Если все настроено верно, то аутентификация должна пройти в штатном режиме, а пользователь должен получить доступ к беспроводной сети.



ИТОГ

Используя NETGEAR ProSAFE WC7520 Wireless Controller мы смогли настроить внешний сервер аутентификации, в роли которого выступал сервер Active Directory. Централизованная база данных AD в связке с контроллером NETGEAR ProSAFE WC7520 это быстрый и эффективный способ применять гранулярные политики безопасности к разным группам пользователей, тем самым обеспечивая для них соответствующий уровень доступа.