

# LAB7: SECURITY & WIRELESS

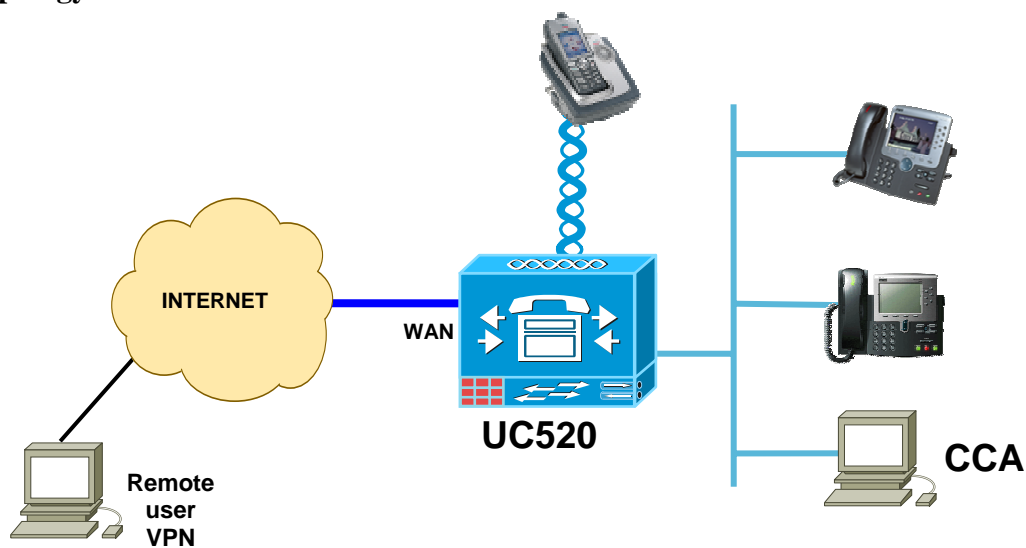
## Introduction:

UC520 is part of the SBCS (Smart Business Communications System) family of products. In addition to its role as an IP phone system for a customer, it also provides Wireless, VPN & Security services.

## Objective:

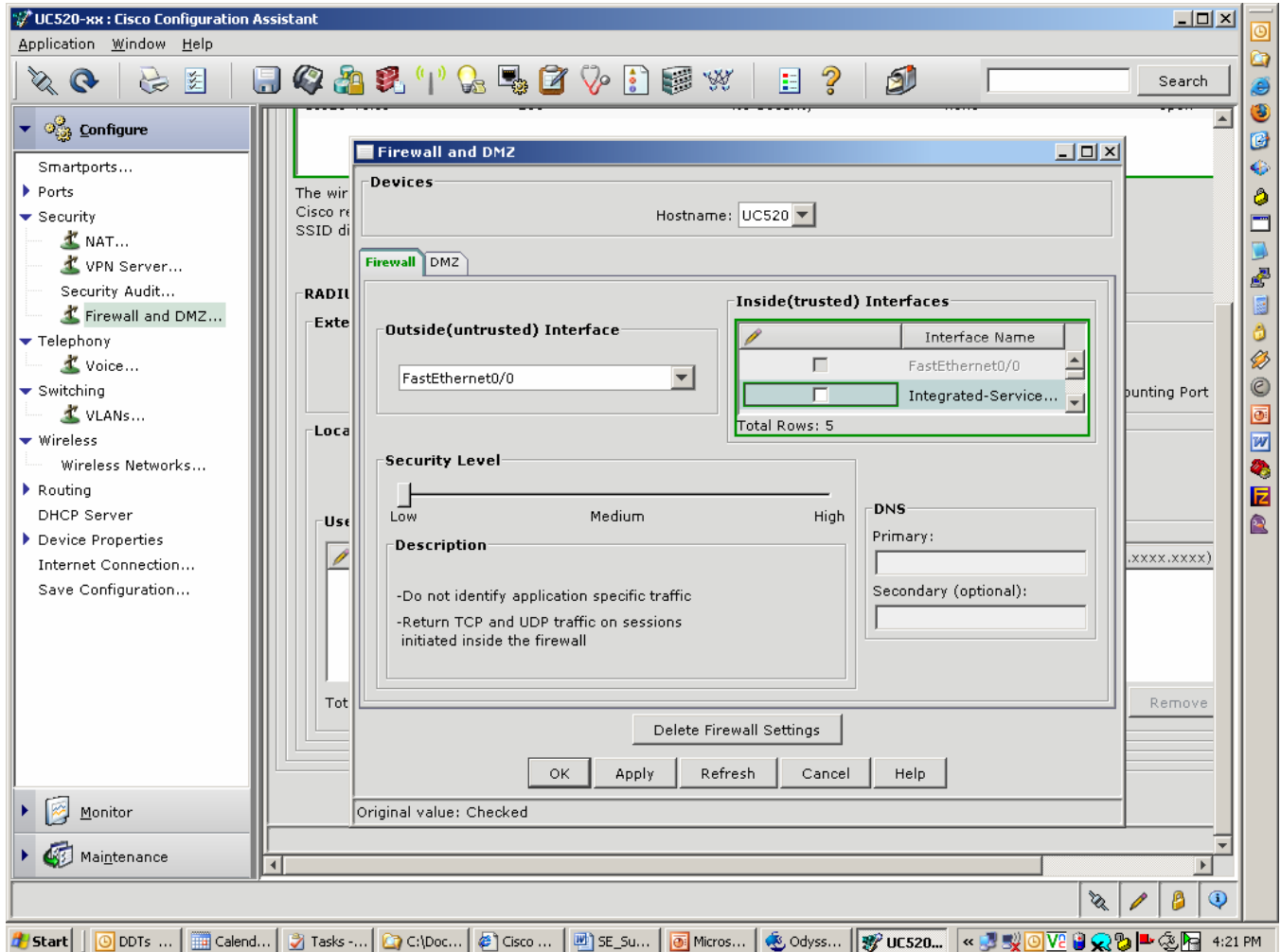
The main objective of this lab is to configure the basic Wireless & Security features. These features will be configured using Cisco Configuration Assistant (CCA). At the end of this lab, a user should be able to configure a WiFi IP phone and also configure VPN access for remote teleworkers to access the internet.

## Topology:

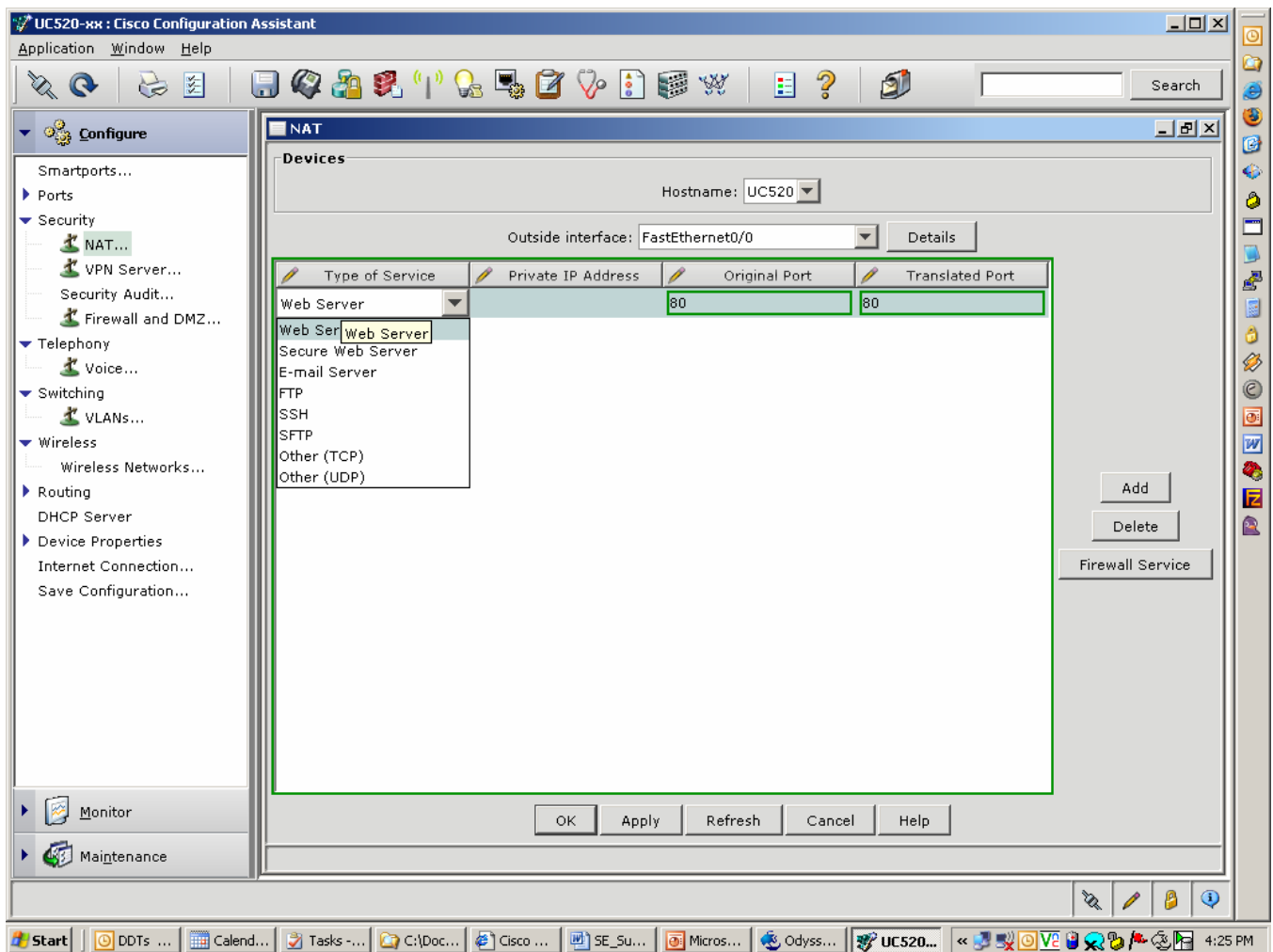


## Setup Steps:

1. Open CCA and login.
2. Click on **Security -> Firewall and DMZ** – change the firewall setting from Low to Medium.  
Notice the description changes as you move the bar. Click on “OK” to apply the change.



- Go to NAT and add static NAT entry for **WEB (HTTP) port 80**. Set the Private IP address to be **192.168.10.100** which is a (simulated) web server. Click on "OK" to apply the change.



#### 4. Click on VPN Server & create EZVPN account

username **cisco123**

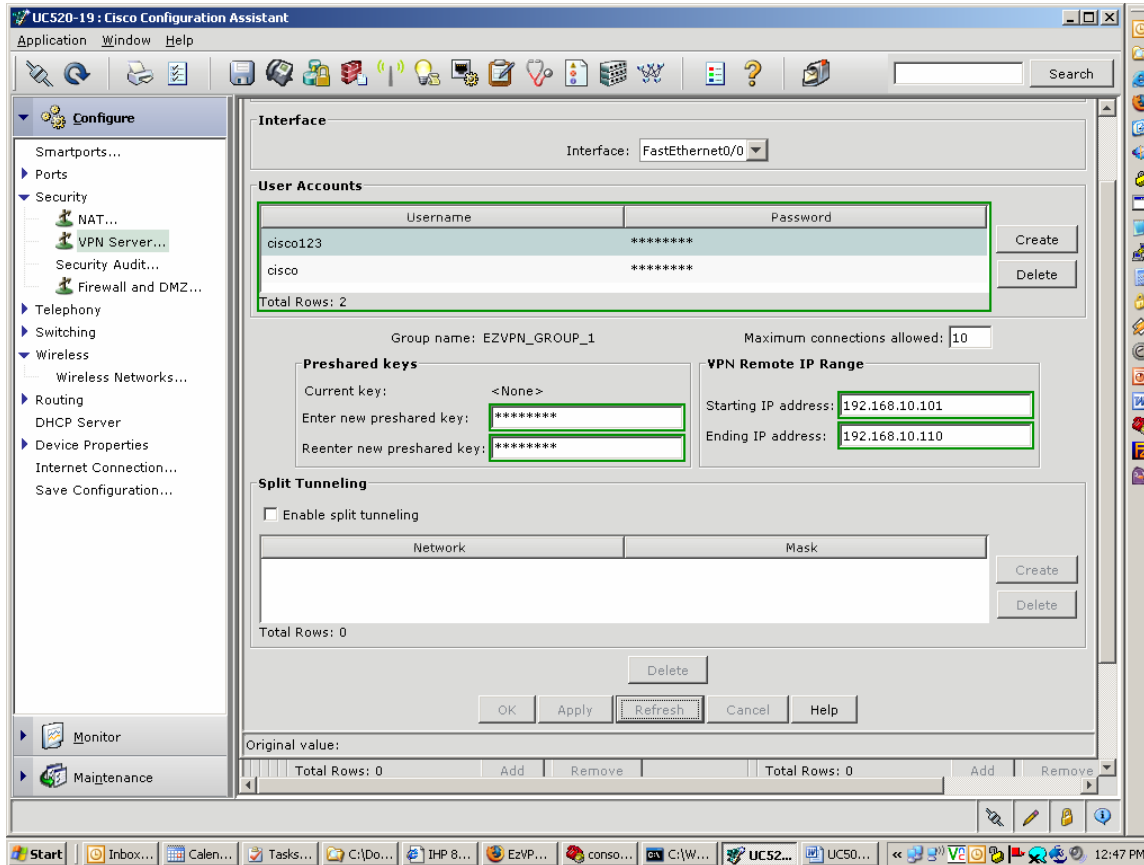
password **cisco123**

Pre shared key **cisco123**

Starting IP address **192.168.10.101**

Ending IP address **192.168.10.110**

Click on “OK” to save changes.



**Verification** - Connect your laptop to the available “broadband internet” connection at your pod. Verify that you get an IP address in the 1.1.100.1xx range. Using your installed VPN client, create a profile for the UC500 and see if you can open a VPN connection to it.

Create new connection and add the below:

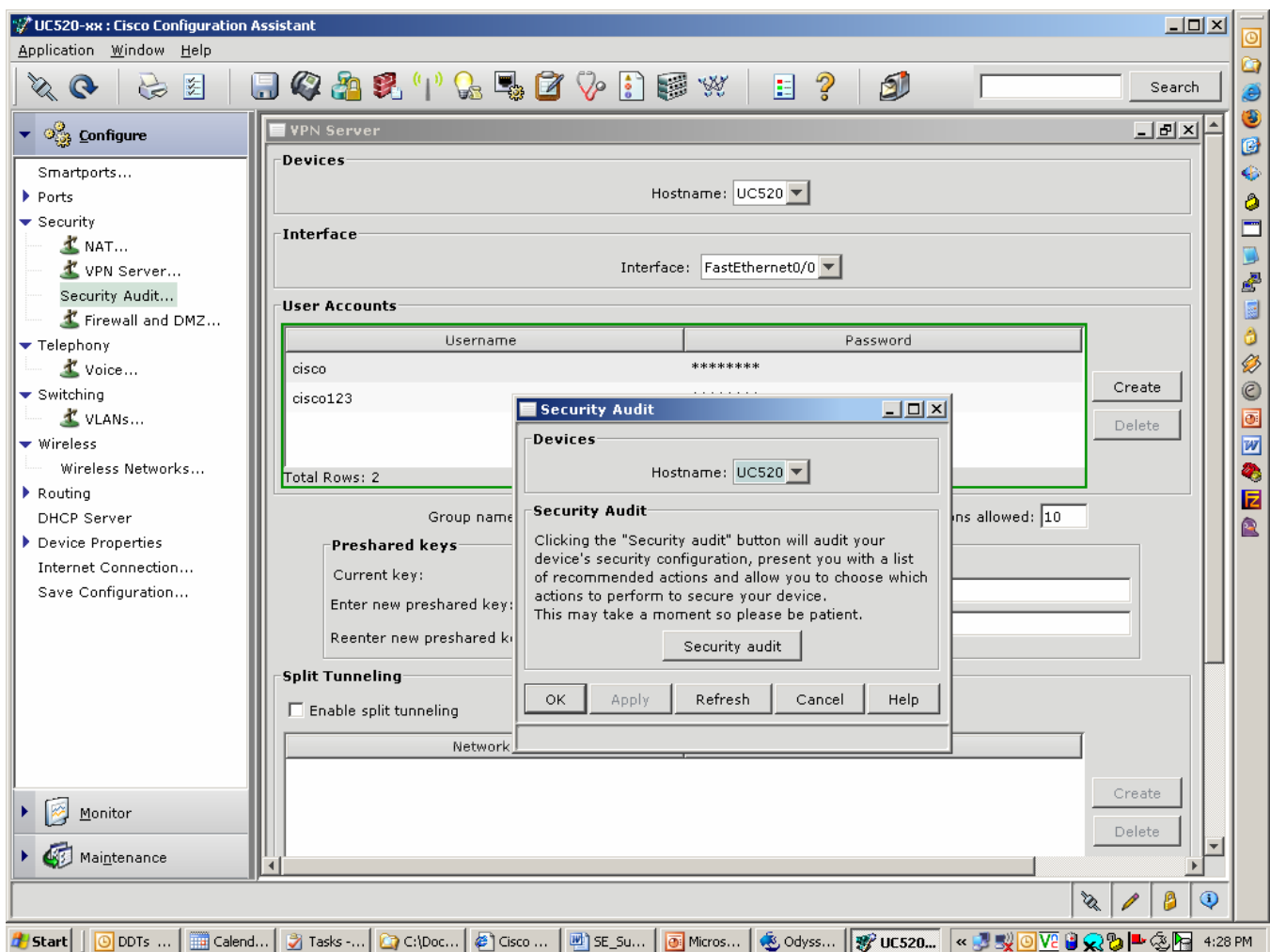
Host 1.1.100.xx (xx is your POD# - drop the leading 0 if any)

Name EZVPN\_GROUP\_1

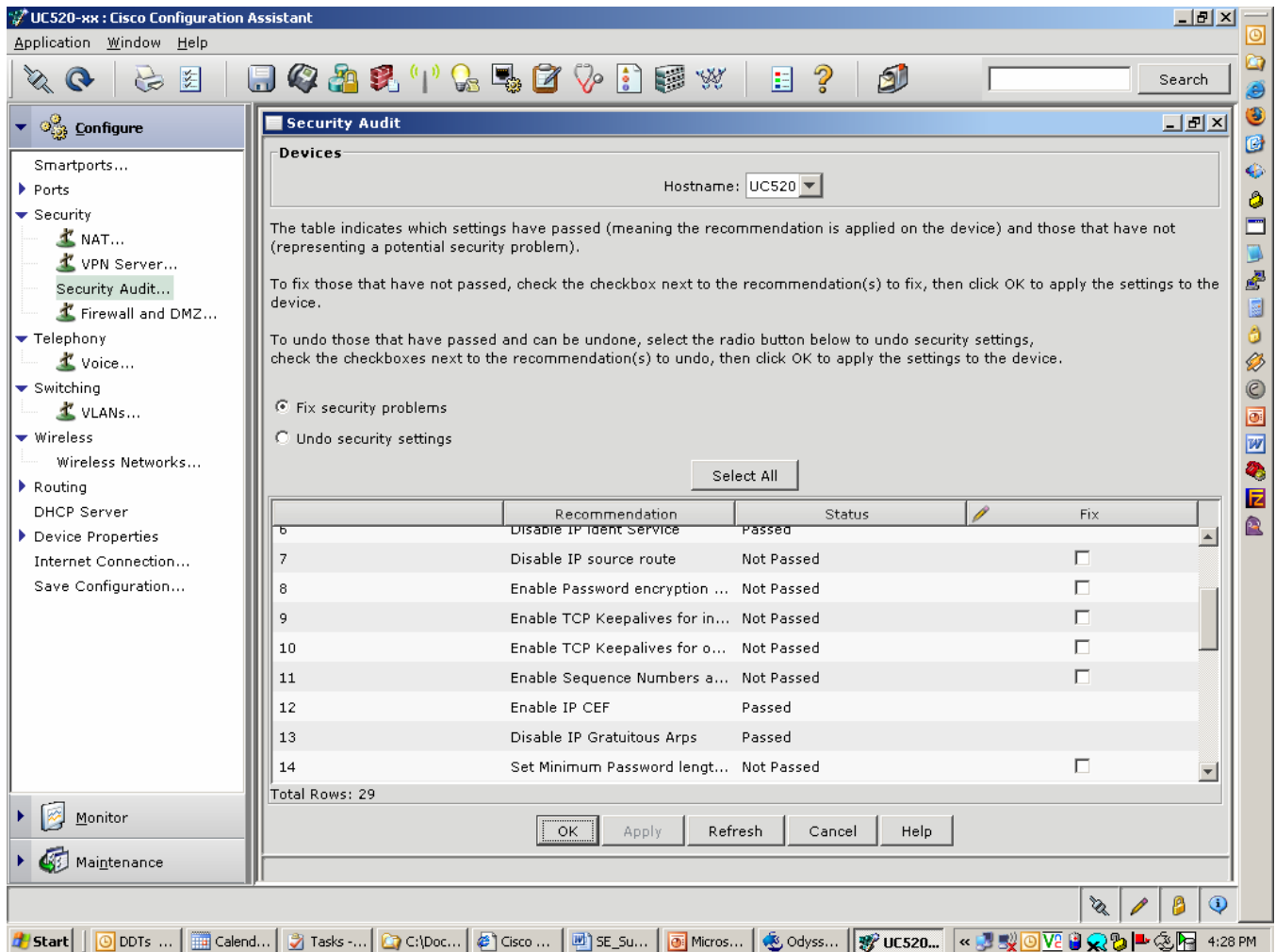
Password cisco123

If the connection is successfully established, you should get an IP address in the 192.168.10.x network. Launch CCA at this time. This emulates the method that would be used to provide remote support to a customer system.

5) Run the security audit feature on CCA as shown below. Note that it may take several minutes to get a response from the audit.



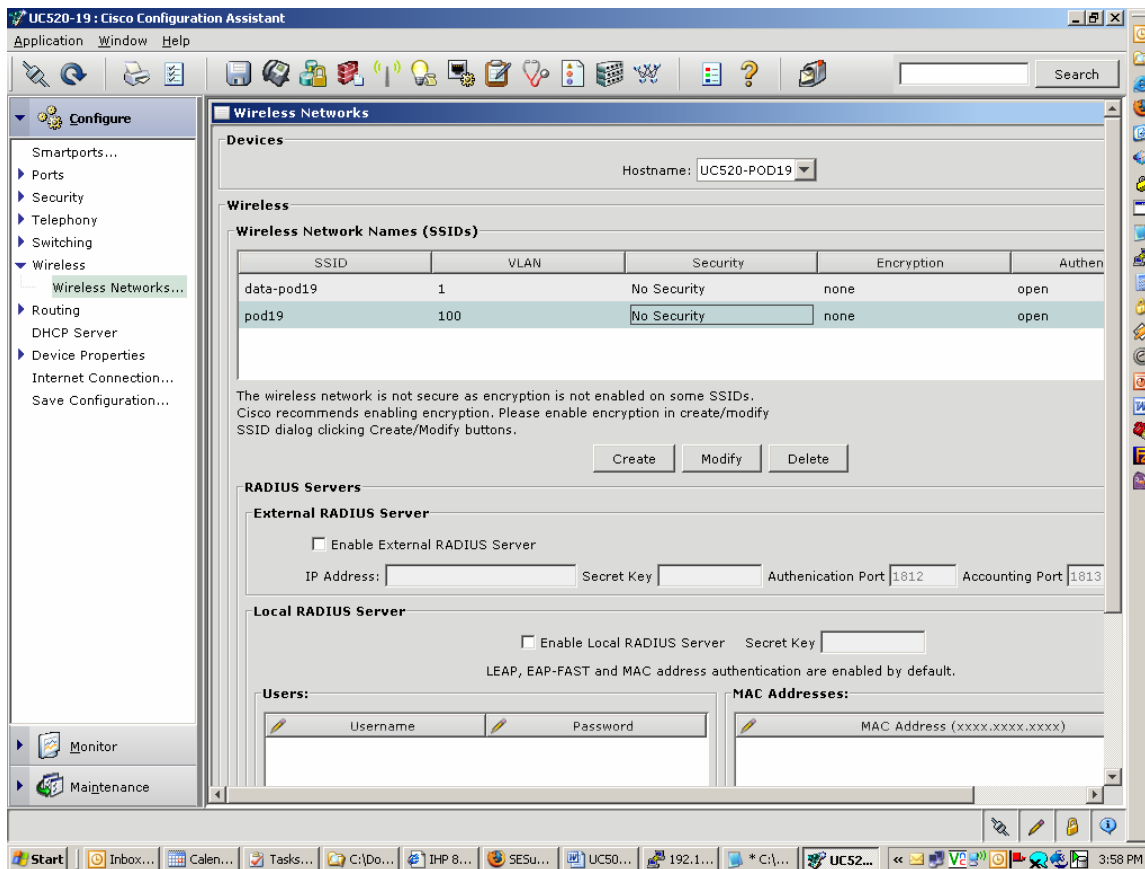
When the audit completes, it will give you a list of potential Security pinholes that may need attention:



Check Disable IP Source route & Enabled password encryption and click on “OK”.

6) For the Wireless section will show how to configure a 7921G IP Phone with SSID podxx (where xx is your pod #).

a) In CCA, click on Wireless -> Wireless Networks



1. Click on the "UC520-Voice" entry and delete it.

Click on "Create" to add a new entry. Make the SSID "podxx" (xx is your POD #). This will be the same SSID used to configure the 7921.

2. Go ahead and enable WEP on the UC520 for the voice SSID – click on podxx and hit modify. Select the below:

Security -> **WEP**

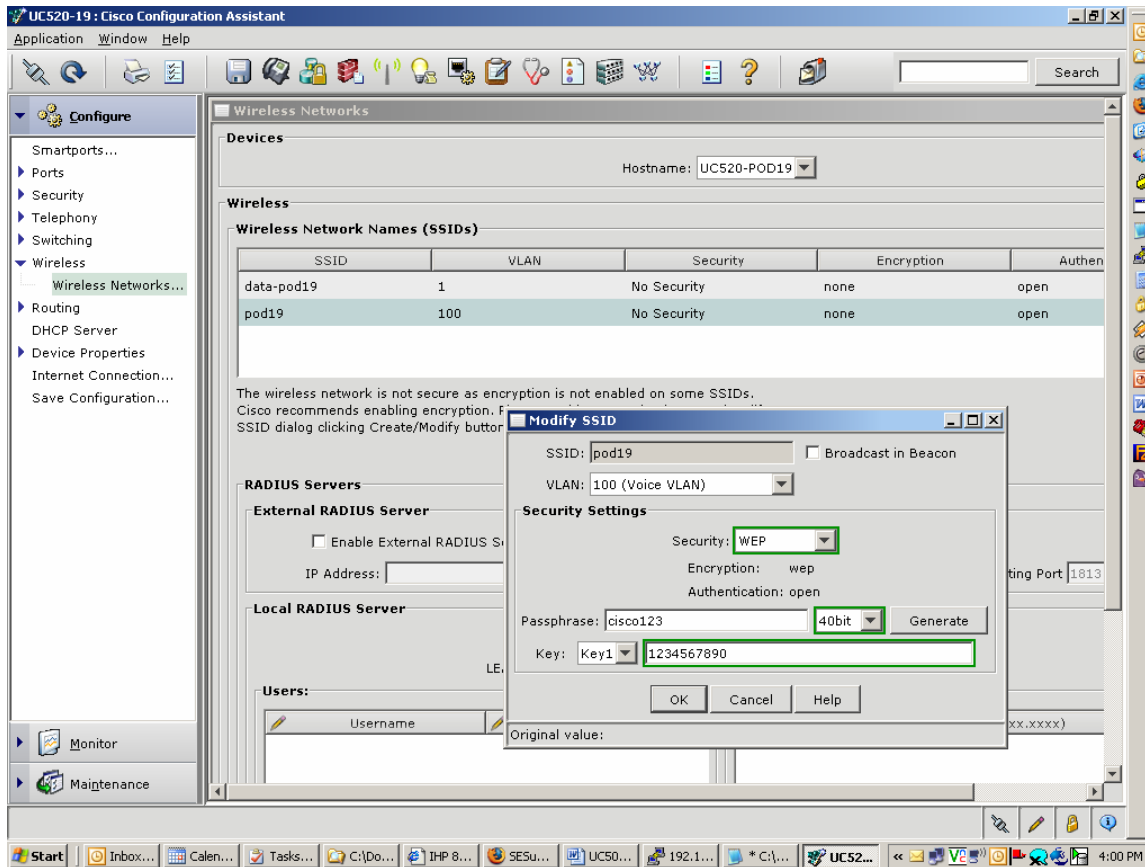
Passphrase -> "cisco123" - select "40 Bit" from the dropdown menu.

3. Click on "Generate". Make note of the generated SSID, as this will be required to configure the 7921 phone.

4. Click on the "UC520-Data" SSID and delete it.

5. Click on "Create" and add an SSID of "podxx-data" on Vlan 1. Ignore the security error warning messages for the lab.

6. Click on "OK" to download the updated configuration to UC520.



- c) Go to the 7921 phone & click on the “down” arrow to enter “settings”
- d) Select Network Profiles and hit “\*\*#” to Unlock the config
- e) Add a new profile & hit Change
- f) Add a profile name - call it UC520-xx (xx is your POD #)
- g) Go to WLAN configuration:  
 add SSID -> podxx  
 Security Mode -> Open+WEP  
 Key Style -> HEX  
 Static WEP Key 1 (40 Bits) – enter the WEP that was generated above using the key pad
- h) Hit Options & Save and go back to the Main Screen
- i) You should see the 7921 register to the UC520 with an auto assigned extension.

You can test calls to/from the wireless phone to verify correct operation.

**NOTE: When both you have completed this lab, please reset UC500 and CUE to factory default setting using the procedure in [Appendix A](#)!**