

HOWTO: ZeroShell WPA Enterprise  
by Paul Taylor

ZeroShell can be obtained from:  
<http://www.zeroshell.net/eng/>

For my installation, I created a VMware virtual machine with 128 MB of ram and a .1 GB hard drive (102 MB).

After the VM boots up, set your local NIC to an IP Address on the 192.168.0.X network, such as 192.168.0.99 and navigate to <http://192.168.0.75> in your browser.

Login as admin with the password of zeroshell.



ZEROSHELL  
Net Services

X.509 certificates  
[CA](#) [Users](#) [Hosts](#) [CRL](#)


Username

Password

### Set up the ZeroShell Database

Note: If you already have a ZeroShell database, skip to the **Create a new CA** section.

After logging in, select the Storage tab:



Release 1.0.beta4  
[About](#)

[Logout](#) [Reboot](#) [Shutdown](#)

CPU ( 1) Intel(R) Celeron(R) CPU 1.80GHz  
1799MHz  
Uptime 0 days, 0:5  
Load Avg 0.15 0.24 0.14

---

SETUP
AutoUpdate
Network
Storage
Time

---

**SYSTEM**

- Setup
- Logs
- Utilities

**USERS**

- Users
- Groups
- LDAP / NIS
- RADIUS
- Captive Portal

**NETWORK**

- Hosts
- Router
- DNS
- DHCP
- VPN
- QoS

**SECURITY**

- Kerberos 5
- Firewall
- X509 CA

**ToDo List**

- Web Proxy
- Wi-Fi AP
- IMAP Server
- SMTP Server

### AutoUpdate Settings

Status: **Active**    Check Interval: 6 hours    Check Now

---

Show All Updates    Last connection: September 21, 2006 19:15

Auto Install    Install

**Available Updates**

Fix ID	Description	Date	Require
No updates available for release 1.0.beta4			

**Installed Updates**    Remove

Fix ID	Description	Date	Required by
No updates installed			

**Message Board**    IT    EN    FR

The site <http://www.zeroshell.net> is unreachable from ZeroShell host 192.168.0.75  
Last Connection: September 21, 2006 21:15

**June 29, 2006**

- \* The ZeroShell Compact Flash Image is available at the URL <http://www.zeroshell.net/eng/download>

**June 25, 2006**


- \* ZeroShell 1.0.beta1 Live CD Image is available at the URL <http://www.zeroshell.net/eng/download>
- \* The Compact Flash Image for devices are able to boot from this media will available within 2 weeks

---

Mar 07 22:04,57 SUCCESS: System successfully started with Linux kernel 2.6.19.3 and ZeroShell 1.0.beta4  
Mar 07 22:09,21 SUCCESS: Session opened from host 192.168.0.1 (Admin)

On this screen, select the hard drive. In this picture, it's "Model: VMware, VMware Virtual S(sda)". This is a virtual SCSI drive.

Note: Both real and virtual IDE drives will have (hda) at the end.



Release 1.0.beta4  
[About](#)

[Logout](#) [Reboot](#) [Shutdown](#)

CPU ( 1) Intel(R) Celeron(R) CPU 1.80GHz  
1799MHz  
Uptime 0 days, 0:5  
Load 0.15 0.24 0.14  
Avg

---

**SYSTEM**

- Setup
- Logs
- Utilities

**USERS**

- Users
- Groups
- LDAP / NIS
- RADIUS
- Captive Portal

**NETWORK**

- Hosts
- Router
- DNS
- DHCP
- VPN
- QoS

**SECURITY**

- Kerberos 5
- Firewall
- X509 CA

**ToDo List**

- Web Proxy
- Wi-Fi AP
- IMAP Server
- SMTP Server

SETUP
AutoUpdate
Network
Storage
Time

Select the disk, partition or database on which you have to operate.

**Warning:**  
This software is NOT guaranteed to be bug free. It is your responsibility to properly test it on scratch disks use it on production devices with important data. In any case, the author is not responsible for any data damage caused by this software.

---

<input checked="" type="radio"/>	Model: VMware, VMware Virtual S(sda)	Capacity:
<input type="radio"/>	Type: ERROR	Capacity: 0 KB

Mar 07 22:04:57 SUCCESS: System successfully started with Linux kernel 2.6.19.3 and ZeroShell 1.0.beta4  
Mar 07 22:09:21 SUCCESS: Session opened from host 192.168.0.1 (Admin)

Once selected, this portion of the screen updates:

Storage Device: sda

**Warning:**

This software is NOT guaranteed to be bug free. It is your responsibility to properly test it on scratch disks before to use it on production devices with important data. In any case, the author is not responsible for any data loss or damage caused by this software.

<input checked="" type="radio"/>	Model: VMware, VMware Virtual S(sda)	Capacity: 102 MB
<input type="radio"/>	Type: ERROR	Capacity: 0 KB

Select "New Partition" and you will get this pop-up:

## VMware, VMware Virtual S (sda)

Refresh Close

Disk /udev/sda: 107 MB, 107374080 bytes  
64 heads, 32 sectors/track, 102 cylinders  
Units = cylinders of 2048 \* 512 = 1048576 bytes

### Partition Size

Fixed Size  GB   
 Max Available

Label

### Filesystem type

Format now  
 Extended 3 (journaled)  
 Reiserfs (journaled)  
 Extended 2 (unjournaled)  
 FAT 32 (unjournaled)

Enter a label and hit Create Partition. When it is done, the screen will refresh.

Now, select "sda1" and you'll get this screen update:

Partition: sda1

### Warning:

This software is NOT guaranteed to be bug free. It is your responsibility to properly test it on scratch disks before to use it on production devices with important data. In any case, the author is not responsible for any data loss or damage caused by this software.

● Model: VMware, VMware Virtual S (sda)		Capacity: 102 MB		
● sda1 ZeroShell	Type: ext3	Capacity: 98 MB	Used: 4127 KB	5%

Select Create DB. You get yet another pop-up. Fill in the Description, Hostname, Realm, LDAP Base, a new Admin password, select a new IP Address/Mask for this Zeroshell installation, and put in your default gateway, like so:

## VMware, VMware Virtual S (sda)

New Database on partition sda1

Create Close

Description	<input type="text" value="ZeroShell"/>
Hostname (FQDN)	<input type="text" value="zeroshell.addressplus.net"/>
Kerberos 5 Realm	<input type="text" value="ADDRESSPLUS.NET"/>
LDAP Base	<input type="text" value="dc=addressplus,dc=net"/>
Admin password	<input type="password" value="*****"/>
Confirm password	<input type="password" value="*****"/>

### NETWORK CONFIG

Ethernet Interface	<input type="text" value="ETH00 - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE] (rev 1)"/>
IP Address / Netmask	<input type="text" value="192.168.111.25"/> / <input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.111.1"/>

Finally, hit Create.

On the next screen, select the newly created database, then the Activate button.

Database: <b>_DB.001 (sda1)</b>	<input type="button" value="Activate"/>	<input type="button" value="Deactivate"/>	<input type="button" value="Info"/>	<input type="button" value="Delete"/>	<input type="button" value="Backup"/>	<input type="button" value="Copy"/>	<input type="button" value="RESCAN"/>
---------------------------------	---	---	-------------------------------------	---------------------------------------	---------------------------------------	-------------------------------------	---------------------------------------

### Warning:

This software is NOT guaranteed to be bug free. It is your responsibility to properly test it on scratch disks before to use it on production devices with important data. In any case, the author is not responsible for any data loss or damage caused by this software.

<b>Model: VMware, VMware Virtual S(sda)</b>		<b>Capacity: 102 MB</b>						
<input type="radio"/> <b>sda1</b> ZeroShell	<b>Type: ext3</b>	Capacity: 98 MB	Used: 4833 KB 6%					
	<table><thead><tr><th>Database</th><th>Description</th><th>Last Activation</th></tr></thead><tbody><tr><td><input checked="" type="radio"/> <b>_DB.001</b></td><td>ZeroShell</td><td>Never</td></tr></tbody></table>	Database	Description	Last Activation	<input checked="" type="radio"/> <b>_DB.001</b>	ZeroShell	Never	
Database	Description	Last Activation						
<input checked="" type="radio"/> <b>_DB.001</b>	ZeroShell	Never						

Another pop-up:

## VMware, VMware Virtual S (sda)

Database \_DB.001 on partition sda1

Activate

Close

### DATABASE INFO

Status: **NOT ACTIVE**

---

Description	: ZeroShell
HostName	: zershell.addressplus.net
K5 Realm	: ADDRESSPLUS.NET
LDAP Base	: dc=addressplus,dc=net
Last Activation	: Never
Last Backup	: Never

---

Net Info

**Warning:** after the database activation the system will be rebooted. This https connection will be closed and network interfaces, routing, firewall, VPNs and VLANs will be reconfigured. As a result, you could be not able to connect to the web interface and could need to put the system into Fail-Safe mode using the local console. For these reasons, you should never activate a new database if you have not access to the console.


Hit the Activate button in this pop-up, then type "Yes" when prompted with the "Are you sure?" question. Your Zeroshell will reboot and come back with the new network settings you gave it.

Note: At this time, if you are using VMware, you will need to modify your VM via the BIOS to boot from CDROM before the hard drive.. Otherwise, it just hangs on reboot, trying to boot from the virtual hard drive.

#### Create a new CA:

After a few minutes the boot will be complete. Navigate to the HTTPS page via the new IP Address you selected and login as admin with your new password.

After you are logged in, select the X509 CA menu item on the left side of the web interface.



Release 1.0.beta4  
[About](#)

[Logout](#) [Reboot](#) [Shutdown](#)

CPU ( Intel(R) Celeron(R) CPU 1.80GHz  
1) 1799MHz  
Uptime 0 days, 0:2  
Load Avg 0.54 0.40 0.16

**X509 CERTIFICATION AUTHORITY**    [List](#)    [Manage](#)    [CRL](#)    [Imported](#)    [Trusted C](#)

Total entries: **2**     Users Certificates     Hosts Certificates     Only not valid Certificates    [Creat](#)

	Common Name (CN)	Serial	Type	Validity Status	Expire
<input type="radio"/>	admin	32138 (0x7d8a)	user	OK	Mar 6 21:2
<input type="radio"/>	zeroshell.addressplus.net	32137 (0x7d89)	host	OK	Mar 6 21:2

Mar 07 22:25,07 SUCCESS: System successfully started with Linux kernel 2.6.19.3 and ZeroShell 1.0.beta4

Mar 07 22:26,23 SUCCESS: Session opened from host 192.168.111.99 (Admin)

Select "Setup" across the tab bar.

CA Certificate and Private Key

[Generate](#)
[Export](#)
 Key
 PEM

Common Name	ZeroShell Example CA	
Key Size	1024 bits	
Validity (Days)	3650	Expire: Mar 13 18:34:37 2016 GMT
Country Name	IT	Status: OK
State or Province		
Locality		
Organization	Zeroshell.net	
Organizational Unit	Example	
E-Mail Address	Fulvio.Ricciardi@zeroshell.	

**Importing CA from external source**    [Import](#)

Private Key    [Choose File](#)    no file selected

Certificate    [Choose File](#)    no file selected

---

**CA Default Parameters**    [Apply](#)

Key Size    1024 bits

Certificate Validity (days)    365

Here, you define your own CA. Note that some characters are forbidden, but the interface doesn't let you know what went wrong. Instead, items seem to return to the above defaults. Here are my working selections:


CA Certificate and Private Key		Generate	Export	<input checked="" type="checkbox"/> Key	PEM
Common Name	<input type="text" value="AddressPlus CA"/>				
Key Size	<input type="text" value="1024 bits"/>				
Validity (Days)	<input type="text" value="3650"/>	Expire: Mar 4 21:32:01 2017 GMT		Status: OK	
Country Name	<input type="text" value="US"/>				
State or Province	<input type="text" value="FL"/>				
Locality	<input type="text" value="Jacksonville"/>	<b>Importing CA from external source</b>		<input type="button" value="Import"/>	
Organization	<input type="text" value="Addressplus.net"/>	Private Key	<input type="button" value="Choose File"/>	no file selected	
Organizational Unit	<input type="text" value="AddressPlus"/>	Certificate	<input type="button" value="Choose File"/>	no file selected	
E-Mail Address	<input type="text" value="ptaylor@addressplus.net"/>				
<b>CA Default Parameters</b>		<input type="button" value="Apply"/>			
Key Size	<input type="text" value="1024 bits"/>				
Certificate Validity (days)	<input type="text" value="365"/>				

After entering your settings, hit "Generate", then OK on the "Are you sure" dialog. When the screen returns, ensure that all your fields are correct.

#### Create users

Next, go to the Users item on the left pane of the web interface.





Release 1.0.beta4  
[About](#)

CPU ( Intel(R) Celeron(R) CPU 1.80GH:  
 1) 1799MHz  
 Uptime 0 days, 0:2  
 Load Avg 0.54 0.40 0.16

[Logout](#) [Reboot](#) [Shutdown](#)

**SYSTEM**

- Setup
- Logs
- Utilities

**USERS**

- Users
- Groups
- LDAP / NIS
- RADIUS
- Captive Portal

**NETWORK**

- Hosts
- Router
- DNS
- DHCP
- VPN
- QoS

**SECURITY**

- Kerberos 5
- Firewall
- X509 CA

**ToDo List**

- Web Proxy
- Wi-Fi AP
- IMAP Server
- SMTP Server

**USERS**

Entries found: **1**

Primary Group

	Username	Group	Description
<input type="radio"/>	admin	0	System Administrator

Mar 07 22:32,04 SUCCESS: CA's private key and X.509 certificate successfully generated

Mar 07 22:32,06 SUCCESS: ZeroShell host certificate successfully generated

Add your new user, tabbing between all the fields so that things like Home Directory, and Description will be filled in for you, based on other fields. At the bottom, enter the users password and confirm it before hitting "Submit".

**(New User)**

---

**Account**

Username <input type="text" value="paul"/>	UID <input type="text"/>	Primary Group <input type="text" value="0"/>	GID <input type="text"/>
Home Directory <input type="text" value="/home/paul"/>	Default Shell <input checked="" type="radio"/> bash <input type="radio"/> sh <input type="radio"/> tcsh <input type="radio"/> other <input type="text" value="/bin/bash"/>		

---

**User Information**

Firstname <input type="text" value="Paul"/>	Lastname <input type="text" value="Taylor"/>	Organization <input type="text"/>
Description <input type="text" value="Paul Taylor"/>	E-Mail <input type="text"/>	Phone <input type="text"/>

---

**User Password**

Password <input type="password" value="*****"/>
Confirm <input type="password" value="*****"/>

**Enabled Services**

Kerberos 5 Authentication <input type="checkbox"/>
Host-to-Lan VPN (L2TP/IPsec) <input type="checkbox"/>
802.1X Access ( VLAN <input type="text"/> ) <input type="checkbox"/>

Assuming you entered all the required fields, you should get a screen back showing the certificate. Keep adding until you have all your users.

## Configure RADIUS

Next, hit the RADIUS item on the left navigation.

**Zeroshell** Net Services | Release 1.0.beta4 | About | Logout | Reboot | Shutdown | CPU (1) Intel(R) Celeron(R) CPU 1.80GHz 1799MHz | Uptime 0 days, 0:2 | Load Avg 0.54 0.40 0.16 | Refres

**RADIUS** | Manage | Access Points | Proxy

### RADIUS Server for Wireless and Port Based Network Access Applications

Status: **ACTIVE** |  Enabled | Show Requests | 802.1

**802.1x Configuration** | Save | Cancel

**X.509 Host Certificate**

Local CA | OU=hosts, CN=zeroshell.addressplus.net

View | Status: **OK** |  Check CRL | Imported | Trusted CA

**Some Notes**

This RADIUS server supports EAP-TLS, PEAP and EAP-TTLS because through TLS they guarantee a strong authentication and management for Wi-Fi Protected Access (WPA). In order to encrypt the communication between the RADIUS server and the clients you need to select an X.509 host certificate and the related private key. EAP-TLS also needs to use X.509 user certificates and related keys on the client-side in order to authenticate the users. In PEAP and EAP-TTLS the only tunnelled authentication supported is MSCHAPv2 that authenticates the clients with the same usernames and passwords used with Kerberos. In any case LDAP user authorization is needed to associate to the WLAN. Don't forget to set a shared secret between Access Points and the RADIUS server in order to permit them to communicate.

Mar 07 22:38,26 SUCCESS: Private key and X.509 certificate successfully generated for paul (user)  
Mar 07 22:38,27 SUCCESS: adding new entry "uid=paul,ou=People,dc=addressplus,dc=net"

Select "Access Points" from the navigation bar across the top.

Add an access point, it's IP Address with a /32, along with a good Shared Secret string.

NOTE: The Shared Secret can not be 32 characters or longer!!! RADIUS will not start with a longer shared secret with the current version of ZeroShell.

### Access Point List

Close

Access Point Name	IP or Subnet	Shared Secret	Add	Change	Delete
<input type="text"/>	<input type="text"/> / <input type="text"/>	<input type="text"/>			

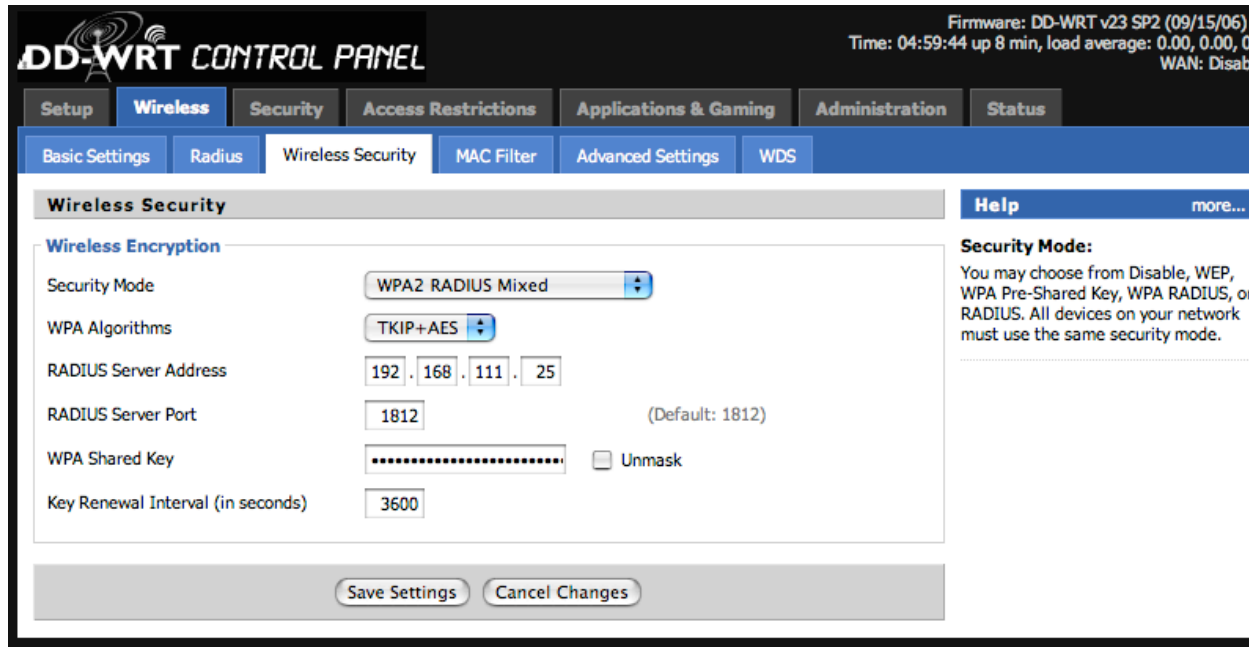
	Access Point Name	IP or Subnet	Shared Secret
<input type="radio"/>	Linksys	192.168.111.5/32	PickAStringLessThan32Characters

After configuring ZeroShell, you should now Reboot it via the link near the top of the screen.

### Configure your Access Point

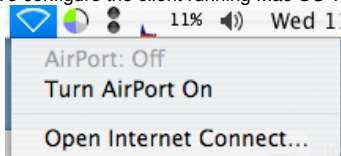
This section varies depending on what AP hardware you have. Basically, you have to turn on RADIUS security, select the appropriate WPA security, point your AP to your ZeroShell IP Address

You must also configure your access point. In this case, I'm running DD-WRT on a Linksys WRT54GS, but it should work fine with the default Linksys firmware. In my case, I've set it to WPA2 RADIUS Mixed mode, which means I can have both WPA and WPA2 clients.

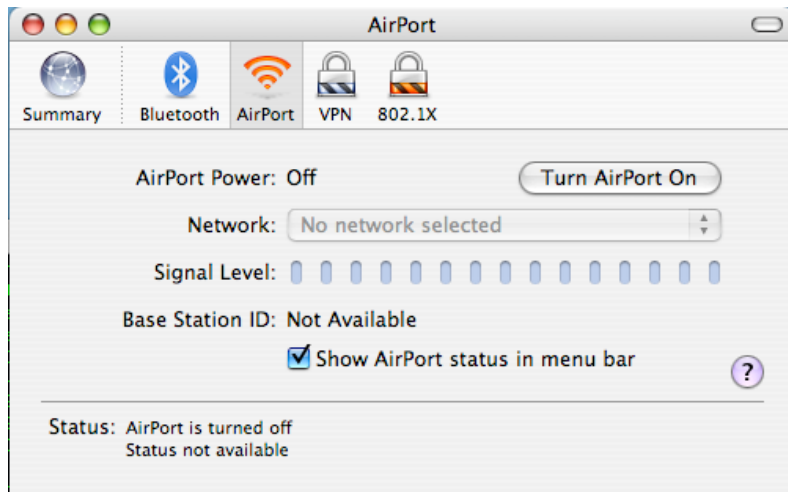


#### Configure a Mac OS X client

To configure the client running Mac OS 10.4, start the "Internet Connect" program.

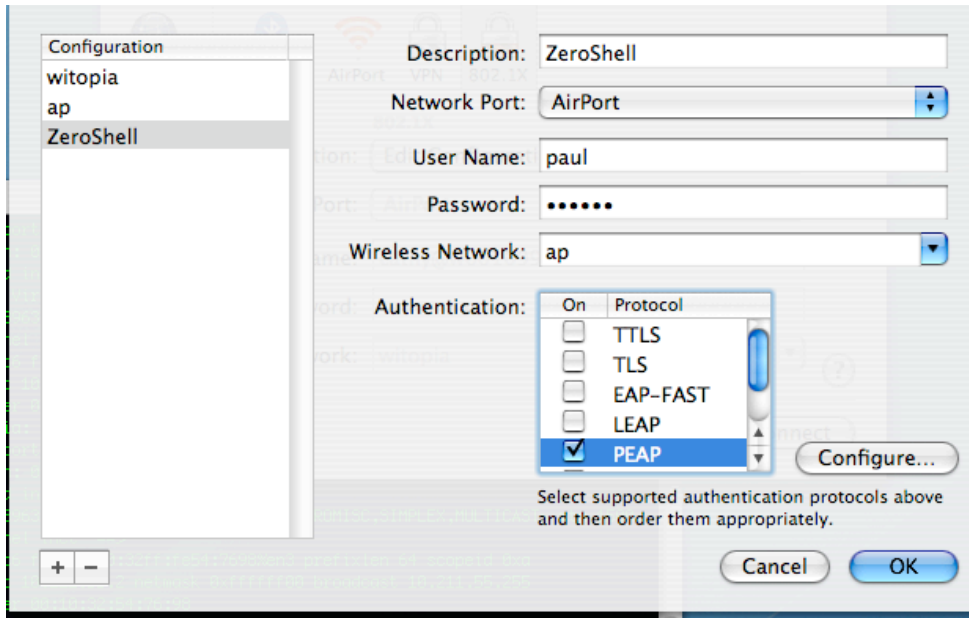


Hit the 802.1X button.

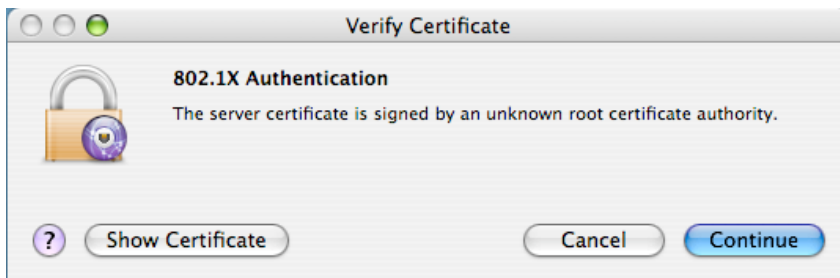


In the Configuration pulldown, select "Edit Configurations".

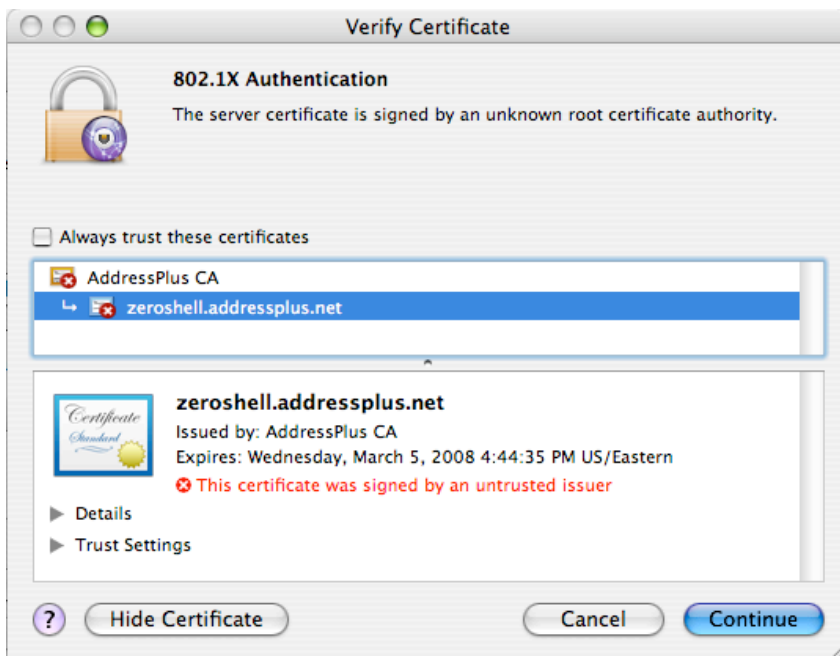
Here, put in a description, add a username and password that you entered earlier, select the SSID of your wireless network, and uncheck all the Authentication boxes except "PEAP". Finally, hit the OK button, as shown below.



Next, Select "ZeroShell" on the Configuration dropdown and hit Connect. (Turn on your Airport, if it is off). You should get this:



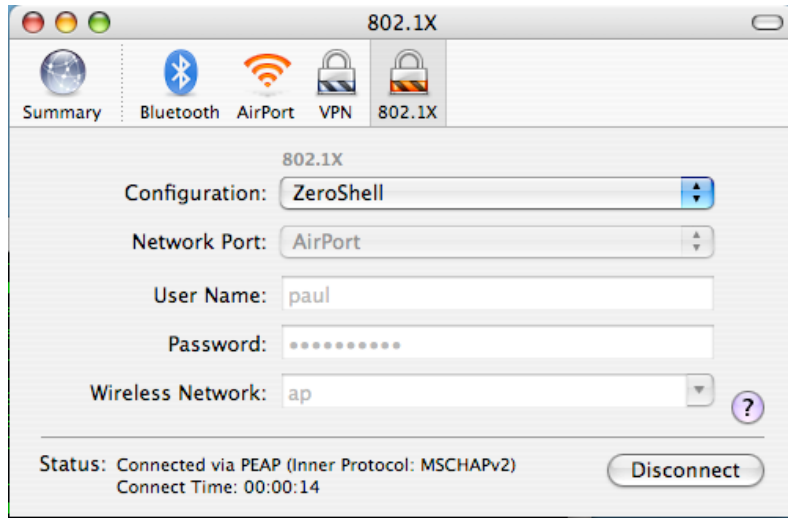
Hit "Show Certificate".



Check the "Always trust these certificates" box and hit Continue.

You should be prompted for your Mac OS password at this time. This is so that the certificate is added as a trusted certificate for future connections.

It should almost immediately move to a Connected state, like so:

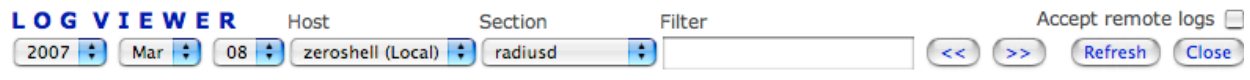


Note the "Connected via PEAP" next to status.

Back in ZeroShell, if you hit "Show Requests" on the Radius screen, you can see your requests via the log functionality of ZeroShell.

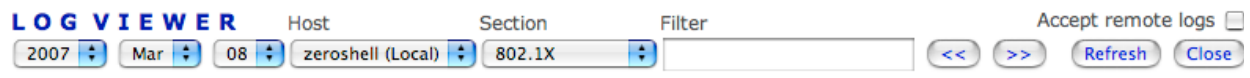
Note: If you skipped the Reboot step earlier, this will not work with the current version of ZeroShell. You must reboot before your logs will show up properly. (You may also be able to restart the Radius server, but I did not test that.)

Here's the "Show Requests" screen:



```
04:55:32 Ready to process requests.
05:01:20 Ready to process requests.
05:12:09 Ready to process requests.
05:12:33 TLS_accept:error in SSLv3 read client certificate A
05:13:33 TLS_accept:error in SSLv3 read finished A
05:13:53 Login incorrect: [paul] (from client Linksys port 36 cli 001451e6dd9f)
05:14:03 TLS_accept:error in SSLv3 read client certificate A
05:14:06 rlm_eap_mschapv2: Issuing Challenge
05:14:06 Login OK: [paul] (from client localhost port 0)
05:14:06 Login OK: [paul] (from client Linksys port 36 cli 001451e6dd9f)
```

And, the "802.1X" log screen:



```
05:14:06 PEAP: "paul" successfully authenticated on Access Point 192.168.111.5
```

### Configure a Windows XP client

First export your CA from ZeroShell.

To do this, go to the Radius screen in ZeroShell and hit the "Trusted CAs" button. That will give you this pop-up:

## Trusted Certification Authorities

View Export PEM Close

### Trusted CAs list

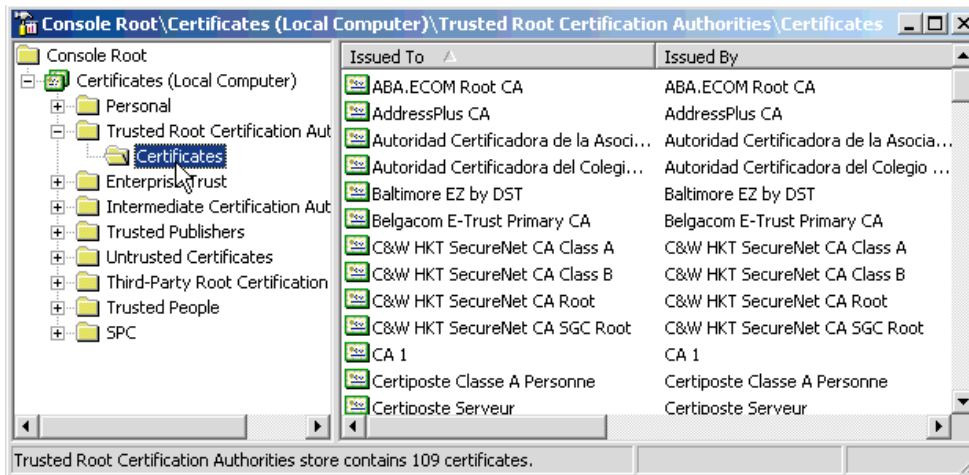
AddressPlus CA/emailAddress=ptaylor@addressplus.net (Local CA)

Import Choose File no file selected Remove

Here, select the CA to export and hit the Export button. Your browser will download a file called "TrustedCA.pem". Copy this file to a USB thumbdrive (or whatever you need to do) to get it over to the Windows machine you want to secure with Enterprise level wireless security.

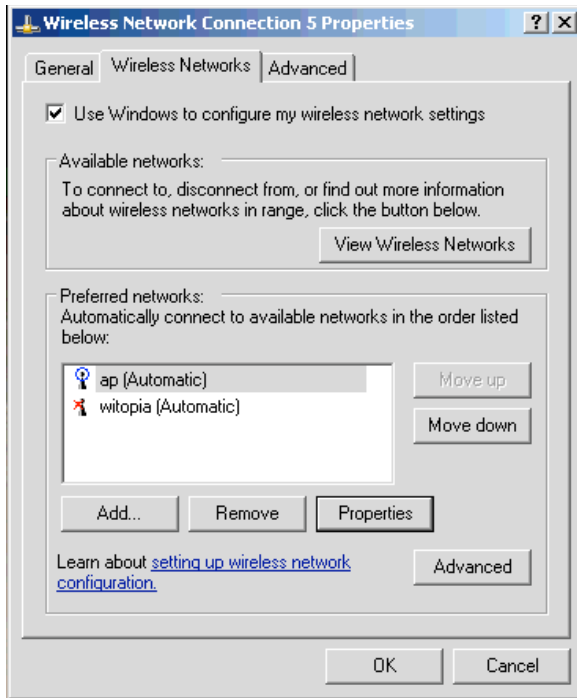
Now, on the windows machine, hit Start, Run, then type in mmc. Hit File, Add/Remove Snap-in, then hit Add and select Certificates. On the next screen, select "Computer account" and "Local Computer" on the screen after that. Next, hit close, then Ok.

Finally, you should have a screen similar to this:

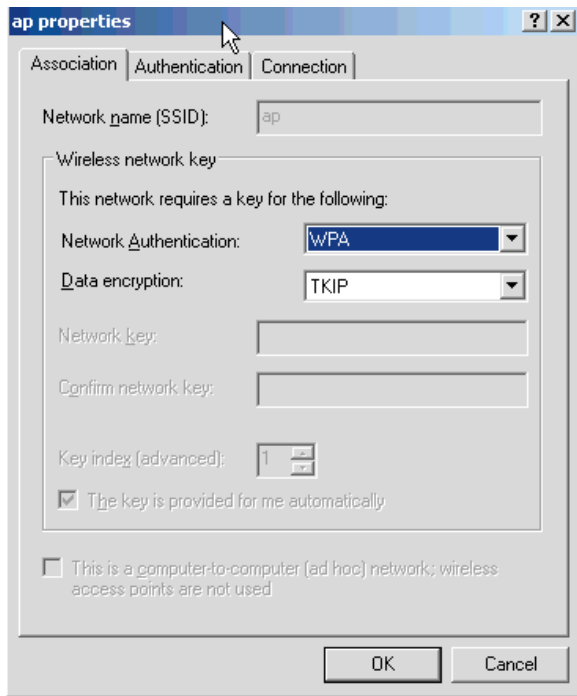


Expand the Trusted Root Certification Authorities, as I've done above. Right click on Certificates, All Tasks, Import. Now, import the certificate file you exported from ZeroShell.

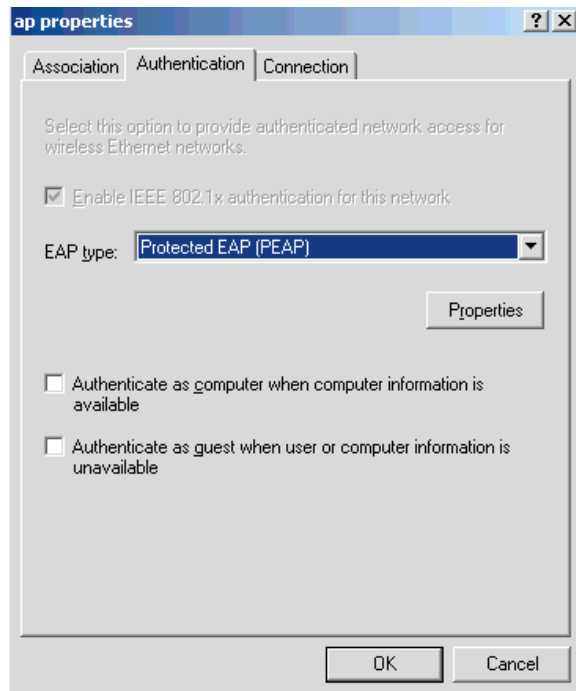
Next, go to the Wireless Networks tab under the properties for your Wireless card:



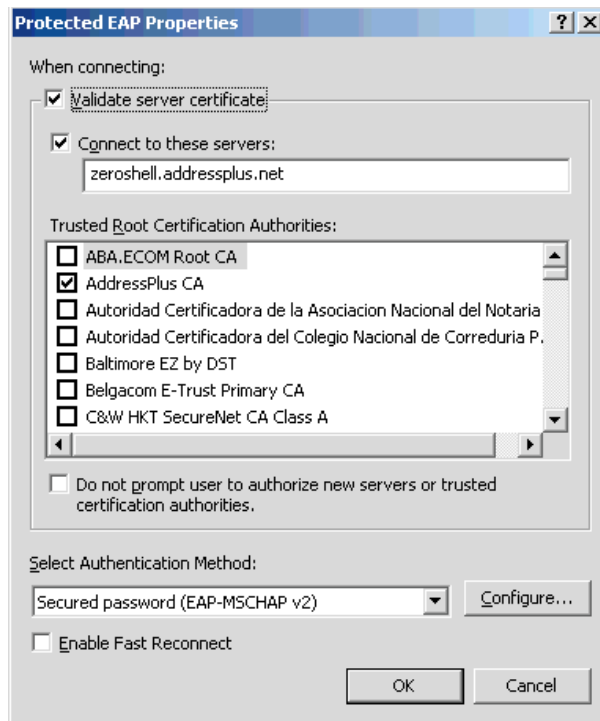
Click the Properties button for the network in question. For Network Authentication, select WPA, and for Data Encryption, select TKIP:



Hit the Authentication tab, check the "Enable IEEE 802.1x" box, and select PEAP for your EAP type. Ensure the other two checkboxes are unchecked:



Select Properties. Select the checkbox for your root CA. In my case, it is AddressPlus CA. Also, set the Authentication Method to MSCHAP:



Hit the Configure button for MSCHAP and ensure that the "Automatically use my Windows logon name and password" box is unchecked.

The first time you try to bring the connection up, you will get prompted for a username and password. Enter the username and password you added to Zeroshell for this computer. You should authenticate successfully.