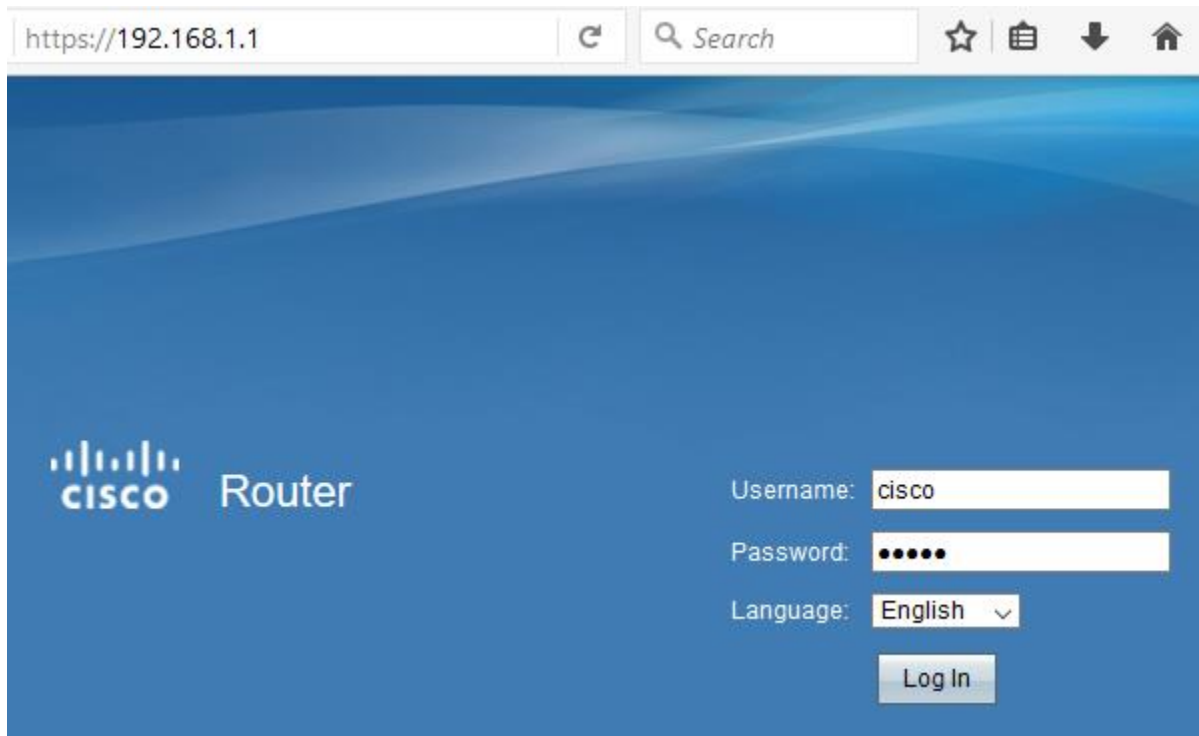



## Initial setup of Cisco RV325 with OpenVPN



https://192.168.1.1

Search

 Router

Username:

Password:

Language:

Login using cisco and cisco

### Change Password

Old Password:

New Password:

Confirm New Password:


Password Complexity Settings:  Enable

Minimal password length:  (Range: 0 - 64, Default: 8)

Minimal number of character classes:  (Range: 0 - 4, Default: 3)

The four classes are: upper case (ABCD...), lower case(abcd...), numerical(1234...) and special characters(!@#\$...).

The new password must be different than the current one:  Enable

Password Strength Meter: 

Change to a simple password as this will be removed soon, click "Save" then login using cisco and the new password.

## Time

Current Time: 2017-07-17, 06:33:27  
Modification time: 2017-07-17, 08:33:27  
Time Zone: Central Time (US & Canada) (GMT-6:00) ▾  
Adjust for Daylight Savings Time:   
Daylight Saving Mode:  By date  Recurring  
From: Month: 06 ▾ Day: 25 ▾ Time: 12 ▾ 00 ▾  
To: Month: 12 ▾ Day: 25 ▾ Time: 12 ▾ 00 ▾  
From: Month: 03 ▾ Week: 2nd ▾ Day: Sun ▾ Time: 02 ▾ : 00 ▾  
To: Month: 11 ▾ Week: 1st ▾ Day: Sun ▾ Time: 02 ▾ : 00 ▾  
Daylight Saving Offset: +60 ▾ Minutes  
Set Date and Time:  Auto  Manual  
NTP Server: time.nist.gov  
Enter Date and Time: 6 hours 33 min 27 sec  
7 month 17 day 2017 year

Set time and date, click "Save"

## My Certificate

My Certificate Table Items 1-1 of 1 5 ▾ per page

Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN- OU=RV325	From: 2012-11-11 To: 2022-11-09		

Page 1 ▾ of 1

This is the current Certificate, notice it is five years old.

## Firmware Upgrade

- Warning**
- . Uploading a previous version of the firmware might cause the device parameters to be reset to factory default values.
  - . Do not power off, reset, or otherwise interrupt the device during a firmware upload. The upload will require a few minutes to complete.
  - . Do not close this window or disconnect any cables from the device during a firmware upload.
  - . It might suspend network traffic during a firmware upload.

Firmware Upgrade from PC

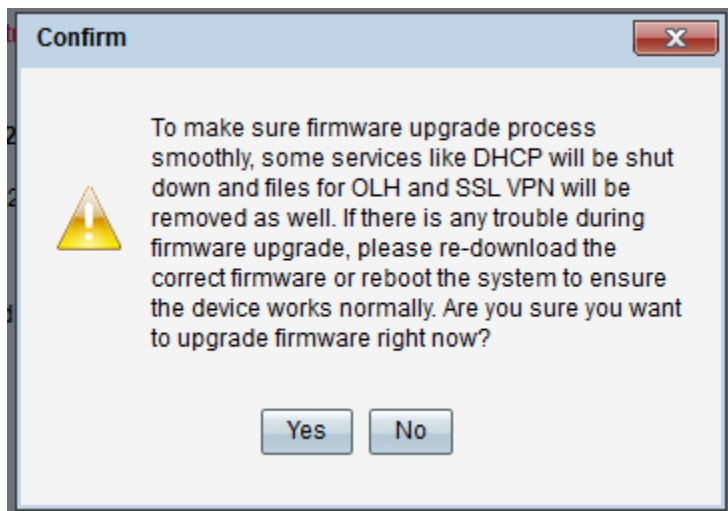
**Firmware Version:** v1.3.1.12 (2016-04-27, 10:46:12)

RV32X\_v1.3.2.02\_20160923-code.bin

Firmware Upgrade from USB

USB Device Status: No Device Attached

Lets get the latest firmware, download and browse to it, the latest is 3.2.02 as of 12/16, click "Firmware Upgrade"



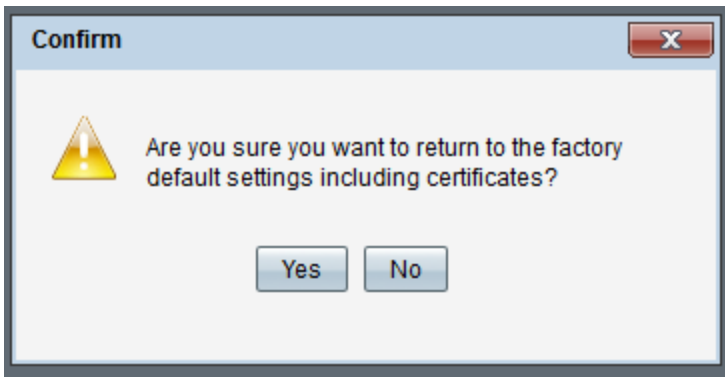
Click "Yes" The red diag light will flash on the router while this is uploading; the router will flash and reset then the diag light will be red while it reboots, this will take about a minute, it will flash again and then the pwr light will be green.

## Factory Default

To reboot the system and return to factory default settings, click 'Factory Default' button.

To reboot the system and return to factory default settings including certificates, click 'Factory Default including Certificates' button.

Now we want to create a new Certificate, click "Factory Default including Certificates"



Click "Yes"



The router will flash and reset then the diag light will be red while it reboots, this will take about a minute, it will flash again and then the pwr light will be green.

### Change Password

Old Password:	<input type="password" value="....."/>
New Password:	<input type="password" value="....."/>
Confirm New Password:	<input type="password" value="....."/>
Password Complexity Settings:	<input checked="" type="checkbox"/> Enable
Minimal password length:	<input type="text" value="8"/> (Range: 0 - 64, Default: 8)
Minimal number of character classes:	<input type="text" value="3"/> (Range: 0 - 4, Default: 3)
The four classes are: upper case (ABCD...), lower case(abcd...), numerical(1234...) and special characters(!@#\$...).	
The new password must be different than the current one:	<input checked="" type="checkbox"/> Enable
Password Strength Meter:	

Now, create a strong password, there is no such thing as overkill, here; use a password manager to create a complex one that cannot be broken easily.

## Time

Current Time: 2017-07-17, 06:33:27  
 Modification time: 2017-07-17, 08:33:27  
 Time Zone: Central Time (US & Canada) (GMT-6:00) ▾  
 Adjust for Daylight Savings Time:   
 Daylight Saving Mode:  By date  Recurring  
 From: Month: 06 ▾ Day: 25 ▾ Time: 12 ▾ 00 ▾  
 To: Month: 12 ▾ Day: 25 ▾ Time: 12 ▾ 00 ▾  
 From: Month: 03 ▾ Week: 2nd ▾ Day: Sun ▾ Time: 02 ▾ : 00 ▾  
 To: Month: 11 ▾ Week: 1st ▾ Day: Sun ▾ Time: 02 ▾ : 00 ▾  
 Daylight Saving Offset: +60 ▾ Minutes  
 Set Date and Time:  Auto  Manual  
 NTP Server: time.nist.gov  
 Enter Date and Time: 6 hours 33 min 27 sec  
 7 month 17 day 2017 year

Set time and date, click "Save"

## My Certificate

My Certificate Table Items 1-1 of 1 5 ▾ per page

Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN= [redacted] OU=RV325	From: 2017-07-17 To: 2027-07-15		

Page 1 ▾ of 1

When we check the new cert, we see it is current, Huzzah!

## WAN Setting Table

Interface	Connection Type:
<input checked="" type="radio"/> WAN1	Obtain an IP automatically
<input type="radio"/> WAN2	Obtain an IP automatically
<input type="radio"/> USB1	3G/4G
<input type="radio"/> USB2	3G/4G

Now we set our static WAN IP address, select the interface and click "Edit"

## Network

### WAN Connection Settings

Interface: WAN1

WAN Connection Type: Static IP

Specify WAN IP Address: 74.125.224.72

Subnet Mask: 255.255.255.0

Default Gateway Address: 74.125.224.1

DNS Server 1: 8.8.8.8

DNS Server 2: 8.8.4.4

MTU:  Auto  Manual 1500 B (Range:68~1500, Default:1500)

Save

Cancel

Back

Enter relevant info and click "Save"

## Certificate Generator

### Certificate Generator

Type: Signed Certificate For Openvpn Server

Country Name (C): United States

State or Province Name (ST): California

Locality Name (L): Irvine

Organization Name (O): Cisco Systems, Inc.

Organizational Unit Name (OU): RV325

Common Name (CN): Office

Email Address (E):

Key Encryption Length: 2048

Valid Duration: 3700 Days (Range: 1-10950, Default: 30)

Root Certificate Authority: 01. Issuer: . Your MAC address - Subject: . Your MAC address

Save

Cancel

Now we want to create an OpenVPN Server Certificate, so select that on the "Type:" dropdown, enter correct info and click "Save"

Notice the "Valid Duration:" is set for 3700 days, this is longer than the main cert so when that is redone, this will be lost so 10950 is unnecessary; same for Client, below.

## Certificate Generator

**Certificate Generator**

Type:

Country Name (C):

State or Province Name (ST):

Locality Name (L):

Organization Name (O):

Organizational Unit Name (OU):

Common Name (CN):

Email Address (E):

Key Encryption Length:



Valid Duration:  Days (Range: 1-10950, Default: 30)

Root Certificate Authority:

Now we want to create an OpenVPN Client Certificate, so select that on the "Type:" dropdown, enter correct info and click "Save"

## OpenVPN Certificate

OpenVPN Certificate Table Items 1-2 of 2  per

Type	Subject	Duration	Details
<input type="radio"/> Server Authorized	CN=Office OU=██████████	From: 2017-07-17 To: 2027-09-03	
<input type="radio"/> Client Authorized	CN=Ed OU=██████████	From: 2017-07-17 To: 2027-09-03	

Page 1 of 1

Now you have a server cert and a client cert for OpenVPN, create additional client certs as needed.

NOTE: you may wish to complete the setup and test the first client before creating other users.

### OpenVPN Server

**Basic Setup**

Enable

Select "Enable" and click "Save"

## OpenVPN Server

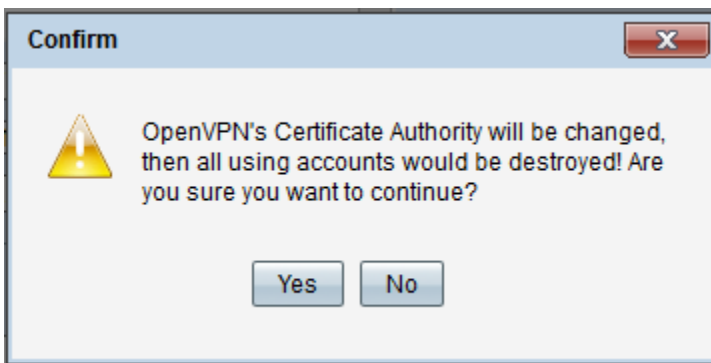
### Basic Setup

Enable	<input checked="" type="checkbox"/>
Authentication:	Password + Certificate
Root Certificate Authority:	01. Issuer: [redacted] Subject: [redacted]
	<input type="button" value="Self-Generator"/>
Server Certificate:	01. Issuer: [redacted] Subject: Office
	<input type="button" value="Generate Certificate"/>
Client Address Pool:	172.31.0.0 (Virtual IPv4 Network Address, Default 172.31.0.0)
	255.255.255.0
Protocol:	TCP
Port:	1194 (Range: 1-65535, Default 1194)
Encryption:	AES-256

### Advanced

Tunnel Mode:	Split Tunnel
Security IP Address:	192.168.1.0
Security Subnet Mask:	255.255.255.0

I change the "Encryption:" to AES-256 and click "Save"



Click "Yes" This is why we flash the firmware and reset with factory defaults before we generate users, etc. 😊



## OpenVPN Account

### User Account Setup

Enable:

Authentication: Password and Certificate

Root Certificate Authority:

01. Issuer: ██████████ - Subject: ██████████

Client Certificate:

02. Issuer: ██████████ - Subject: Ed

Generate Certificate

OpenVPN Server:

██████████ (Name or IPv4 Address)

Username:

Ed

Password:

●●●●●●●●

Save

Cancel

Now we create the user account, select the appropriate Client Certificate, enter a username and password, click "Save"

## Summary

### OpenVPN Tunnel Number

0 Tunnel(s) Used      5 Tunnel(s) Available  
1 Tunnel(s) Enabled      1 Tunnel(s) Defined

### Server Setting Table



	Enable	Authentication	Protocol	Encryption	Client Address Pool
<input type="radio"/>	<input checked="" type="checkbox"/>	Password + Certificate	TCP 1194	AES-256	172.31.0.0 255.255.255.0

Edit

### OpenVPN Account ID Status

#### Account ID Setting Table

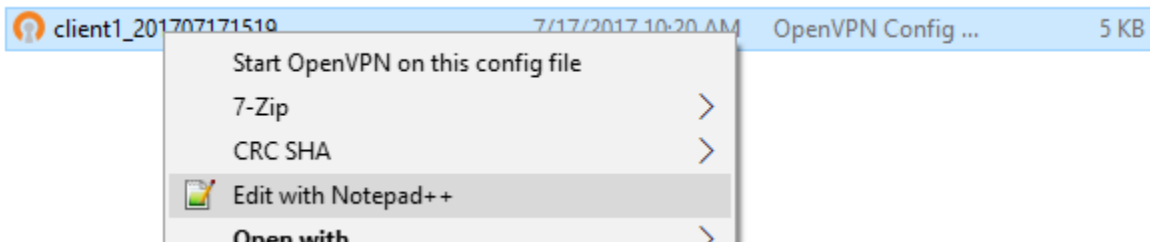
Items 1-1 of 1 5 per p

	Enable	Username	Export .ovpn File	Client Public IP Address	Client Virtual IP Address	Status	Action
<input type="radio"/>	<input checked="" type="checkbox"/>	Ed	 	0.0.0.0	0.0.0.0	Offline	

Add Edit Delete

Page 1 of 1

Download the .ovpn file, I click the OpenVPN icon on the left



I edit with Notepad++

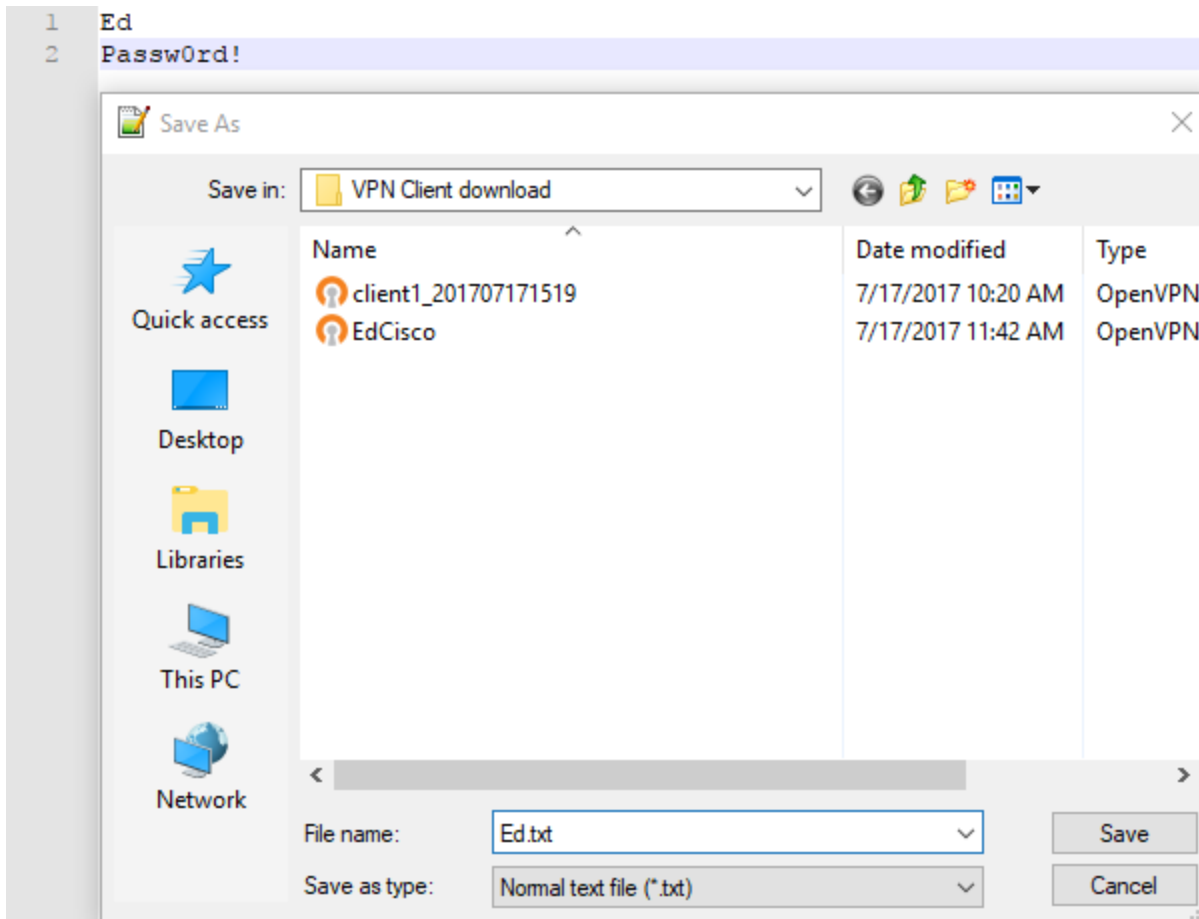
```
1 dev tun
2 proto tcp
3 remote 74.125.224.72 1194
4 cipher AES-256-CBC
5 auth SHA1
6 resolv-retry infinite
7 nobind
8 persist-key
9 persist-tun
10 client
11 auth-user-pass
12 verb 3
13
14 <ca>
15 -----BEGIN CERTIFICATE-----
16 MIIIDvzCCBrOqBwIRBgcLTAQ07n4Nh/r
```

To add my password file into the config, see line 11 above and below

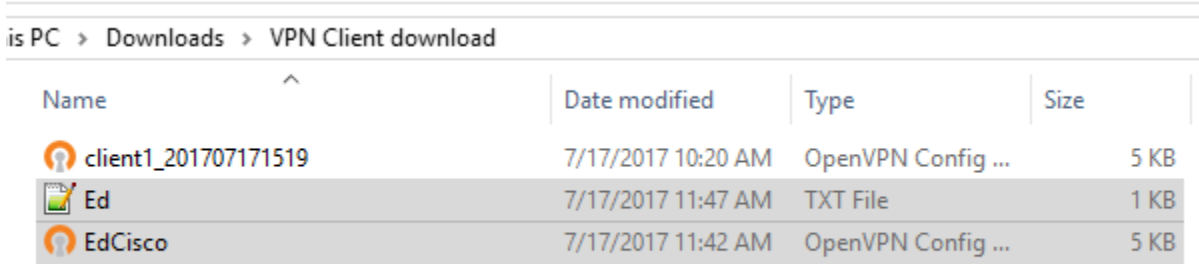
```
1 dev tun
2 proto tcp
3 remote 74.125.224.72 1194
4 cipher AES-256-CBC
5 auth SHA1
6 resolv-retry infinite
7 nobind
8 persist-key
9 persist-tun
10 client
11 auth-user-pass Ed.txt
12 verb 3
13
14 <ca>
15 -----BEGIN CERTIFICATE-----
16 MIIIDvzCCBrOqBwIRBgcLTAQ07n4Nh/r
```

I add the name of the text file with a space after pass.

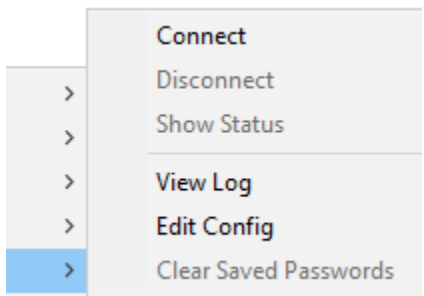
Now save this file as something more easily understood than client\_\*\*\*\*\*.ovpn, such as EdCisco.ovpn



Create and save the password file containing the username and password, name it exactly what appears on line 11 above



Move these two files to... This PC > Local Disk (C:) > Program Files > OpenVPN > config



Now launch OpenVPN and connect to the new network and verify proper operation.