Setting up Time-based One-time Passwords on SonicWall UTM appliances with Google or other Authenticators

SonicWall recently added the ability to integrate their appliances with Time-based Google and other 3rd party authenticators. Time-based passwords generally represent a more cost effective method of generating one time passwords (compared for example to turn-based) and is a method employed by an increasing number of vendors. The following guide assists in deployment of the technology on SonicWall UTM appliances including the NSA and TZ series.

- Make sure that at least 6.5.3.1 Firmware is installed on the SonicWall UTM appliance.

- Ensure the user has installed either Google Authenticator or Microsoft Authenticator (the procedure is the same for each).

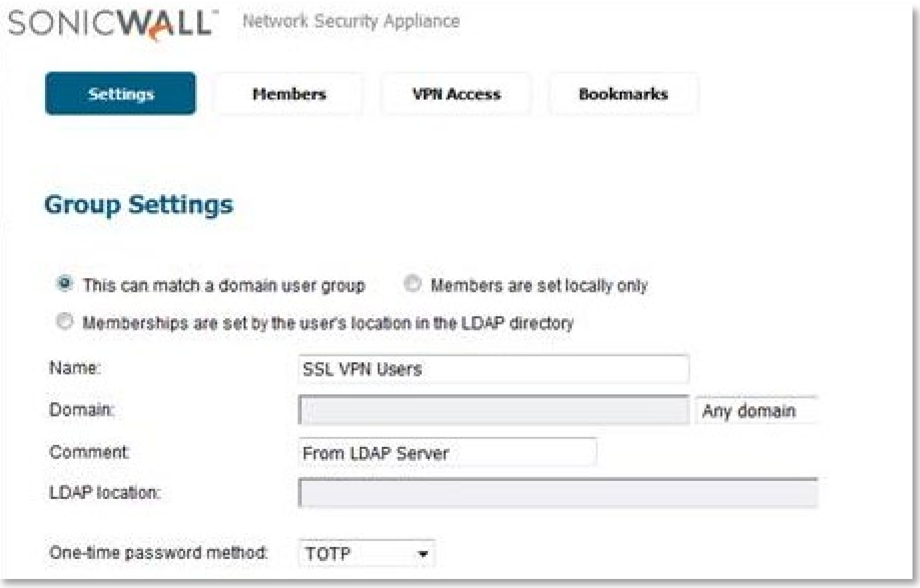
- Set up the relevant Authentication method on the SonicWall either local database, LDAP or Radius.

- Import the User group for the VPN users to the SonicWall so it appears under Local Groups.

- Set up the SSL VPN Feature on the SonicWall. (https://www.sonicwall.com/support/knowledge-base/170505401898786/)

- Get the User to download the relevant SSL VPN client to their device (SonicWall Mobile Connect for Android, iPhone / iPad, Apple OS Maverick +, Windows 8.1 + and) Windows 7, 8.1,10 and Linux can still use the Latest version of Netextender available from Mysonicwall.com.

- Edit the User group on the SonicWall as below and enable TOTP as the One-Time password method and click Apply and Ok.



Group Settings

● This can match a domain user group ○ Members are set locally only

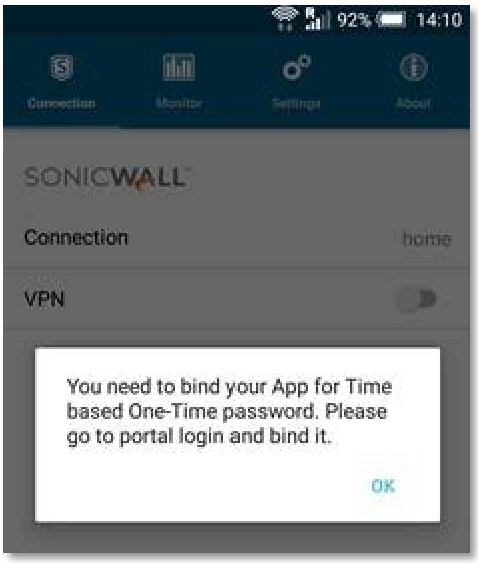
○ Memberships are set by the user's location in the LDAP directory

Name:	SSL VPN Users
Domain:	Any domain
Comment:	From LDAP Server
LDAP location:	
One-time password method:	TOTP

- Get the User to go to https://YourURL:(SSL VPN port if not using 443) the Default it 4433. For the first time this is probably best done on a pc so the user can scan the barcode from the screen if not they can use the Text Code method and copy and paste from the mobile browser in to their chosen authenticator.

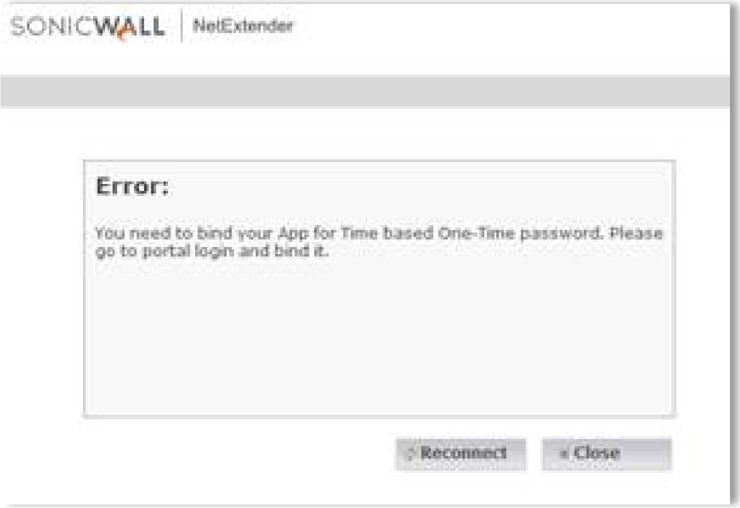
- If they try and login using their SSL VPN client before they will get the error as below.

From Mobile Connect Client



You need to bind your App for Time based One-Time password. Please go to portal login and bind it.

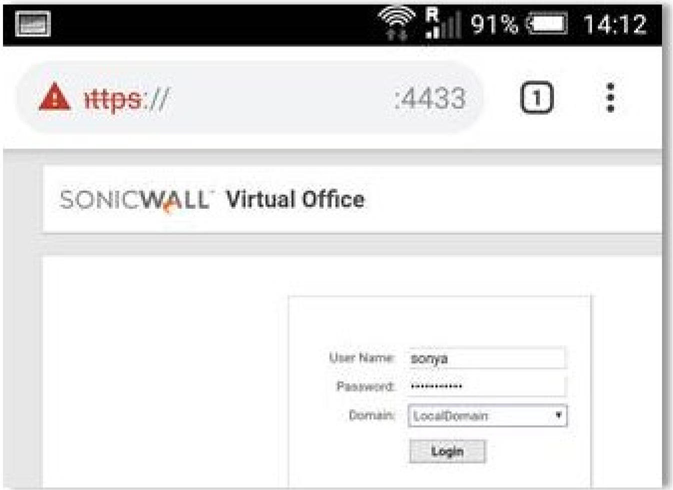
From Netextender Client



Error:

You need to bind your App for Time based One-Time password. Please go to portal login and bind it.

- The User logs in for the first time using the portal



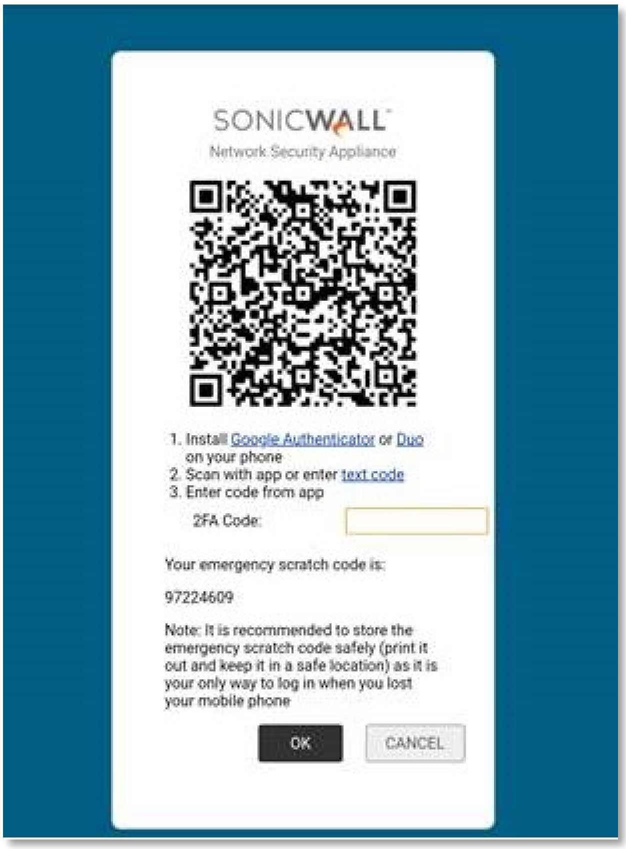
SONICWALL Virtual Office

User Name: sonya

Password: ••••••••••••

Domain: LocalDomain

- The user will get presented with a screen like the below, as mentioned earlier they will need to scan the barcode or enter the Text Code in to their Authenticator App.



SONICWALL

Network Security Appliance

1. Install Google Authenticator or Duo on your phone
2. Scan with app or enter text code
3. Enter code from app

2FA Code:

Your emergency scratch code is:

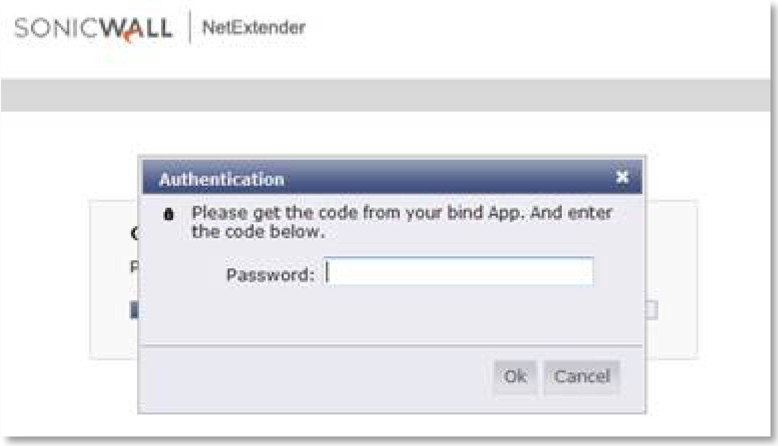
97224609

Note: It is recommended to store the emergency scratch code safely (print it out and keep it in a safe location) as it is your only way to log in when you lost your mobile phone

- Once the User has scanned the code the Authenticator is setup.

- When they next attempt to login using their SSL VPN client after they have entered their login details, they will get a popup like the below.

- They just need to open their Authenticator app and choose the code from the relevant SonicWall Instance (if they are already using App the for Amazon etc…)



Please get the code from your bind App. And enter the code below.

- Once they enter their OTP they will be logged in.

Once the user has completed the OTP set up the User will appear under the SonicWall/Users/Local Users section (don't deleted this as it is keeping all the relevant information regarding their OTP).