



Remote Connection to Your Computers

Accessing files while you're on the go

When you are at home or in the office, your iPad or iPhone connects to your network wirelessly. And because it is part of your network, FileBrowser can directly access any computers and NAS devices on the network. If you have a logon account for a computer, FileBrowser can access it.

But what happens when you're away from home or out of the office? Now you are outside the network, so FileBrowser no longer gets access to network computers or NAS devices. This is because your network is protected by a firewall, usually the one in your internet router.

So how can FileBrowser get through the firewall? There are two methods:

[Port Forwarding](#)

[Virtual Private Networks \(VPNs\)](#)

For most users, the VPN method is more suitable and is also more secure.

Port Forwarding

With this method, you effectively open a 'hole' in your firewall just for FileBrowser. The firewall then allows FileBrowser to connect from the Internet to one specific computer on your network.

This method is simple to set up. First, you add a new rule to your router to send FileBrowser requests straight through your firewall to the target computer. Then you add the router to your Locations list in FileBrowser.

However, this method does come with several risks and restrictions. Learn more about [Port Forwarding](#).

Virtual Private Networks (VPNs)

With this method, you extend your existing home or office network to include remote computers or devices. So your iPad or iPhone can join your network even if it is physically outside the network. And unlike Port Forwarding, a VPN allows FileBrowser to see all the available computers and devices on your network, not just a single computer.

If you want to connect your iPad or iPhone to an existing company VPN, this method is simple to set up. First, you edit the VPN setting on your iPad or iPhone and connect to the VPN. Then you add any target computers to your Locations list in FileBrowser.

If you want to connect to computers or devices on your home network, the setup involves an extra step. First, you set up a VPN server on your home network. Then you edit the VPN setting on your iPad or iPhone. Finally you add any target computers to your Locations list in FileBrowser. Learn more about [Virtual Private Networks](#).

Virtual Private Network (VPN)

With a VPN, you extend your existing home or office network to include remote computers or devices. When your iPad or iPhone connects to your VPN, FileBrowser works exactly the same as if you were at home or in the office, even though you're using 3G or the hotel or coffee shop WiFi to browse the network.

[About VPNs](#)

[How does a VPN work?](#)

[How do I set up a VPN on my home network?](#)

[Add home computers to FileBrowser](#)

[Create a VPN user account](#)

[Install a VPN server](#)

[Configure your router to forward Port 1723 traffic](#)

[Add a new VPN configuration on your iPad or iPhone](#)

[Test the VPN connection over the Internet](#)

[What happens if the IP address changes on my VPN server?](#)

[My VPN still doesn't work!](#)

[Learn more about technical issues.](#)

About VPNs

A virtual private network, or VPN, is an extension to your existing home or office network. It allows remote computers or devices, including your iPad or iPhone, to join your network even if they are physically outside the network. And because all data transferred over a VPN is encrypted, this is the most secure method for remote access.

In simple terms, imagine that your network is like a hotel. Each computer or device on the network is like a hotel room. When you set up a VPN, it is like extending your hotel to include an additional room in a building located in a different city.

A guest in this remote room enjoys all the benefits of being part of the main hotel. In particular, they can use the hotel phone in their room to call any room in the main hotel building. In the same way, when remote computers and devices are connected to your VPN, they can seamlessly connect to any computers on your main network.

How does a VPN work?

To join a VPN, a computer or mobile device uses a *VPN client* to connect to a *VPN server*.

Your iPad or iPhone includes a built-in VPN client. To configure this client, you just edit the VPN settings on the iPad or iPhone. The client can then connect to the VPN server for your network.

When you use FileBrowser on the go to browse a remote network, the VPN client on your iPad or iPhone sends encrypted data to the VPN server. The VPN server then converts this data into internal network requests for files and folders.

If you're connecting to a company VPN

The IT department will have already set up a VPN server. They can give you the details you need. You just need to specify the VPN server in the Settings screen on your iPad or iPhone. Then you simply turn on the VPN setting before you launch FileBrowser.

If you want to connect to your home VPN

First, you set up a VPN server. This can run on any computer on your home network. Then you specify the new VPN server in the Settings screen of your iPad or iPhone. Finally, you simply turn on the VPN setting before you launch FileBrowser.

[Learn more about setting up a VPN on your home network.](#)

How do I set up a VPN on my home network?

Setting up a VPN on your home network involves the following steps. Each step is described fully in the following sections.

1. Add your home computers to FileBrowser.
While at home, launch FileBrowser and add any home computers to the Locations list.
2. Create a VPN user.
This is a standard user account (not an administrator account) that FileBrowser will use to log onto the VPN.
3. Install a VPN server.
You will need to provide details about the VPN user.
4. Configure your router to forward 'Port 1723' traffic to your new VPN server.
5. Edit the VPN settings on your iPad or iPhone.
You must add a new VPN configuration for the VPN server you installed in step 3.
6. Test the VPN.
Can FileBrowser connect to your home computers over the Internet?

Add home computers to FileBrowser

Before you set up a VPN, add your home computers to the Locations list in FileBrowser. Do this using your home WiFi and follow the normal FileBrowser procedure (described below).

When your home VPN is up and running, you will be able to access these same computers over the Internet when you are away from home.

Follow these steps:

1. Verify that your iPad or iPhone is connected to your home WiFi.
2. Launch FileBrowser.
3. Go to the **Scan** page and tap the refresh icon.
4. In the Scan list, tap each computer that appears in the Scan list that you want to connect to and enter your username and password. When FileBrowser offers to remember the computer, select Yes. The computer is added automatically to the **Locations** page.

If the scan doesn't find your computer, add it manually using the following steps.

1. Tap the '+' button in the FileBrowser **Locations** page.
2. In the **New Machine** screen, specify the machine type (typically PC or Mac).
3. In the **Address** field, enter the computer's name or IP address. [Learn more about IP addresses](#).
4. Tap the **Save** button to save the computer details and return to the Locations page.

Select PC, Mac, Time Capsule (AirPort Extreme), NAS Drive or cloud storage

i	PC		✓
i	Mac		
i	TC		
i	NAS		
i	Dropbox		
i	OneDrive		
i	Box		
i	Google Drive		
i	WebDAV		
i	FTP		
i	Point.io		

Enter MY-PC-NAME or SERVER.COMPANY.COM or an IP Address.

i Address Tap here

If you need to supply a User Name and Password for this server, FileBrowser can store these so you don't need to enter them again.

i	User Name	Blank	On demand	Edit...
i	Password	Blank	On demand	Edit...

FileBrowser: Example New Machine screen

Confirm that FileBrowser is able to connect to your computer on your home network before continuing to the next stage

Create a VPN user account

If you use a VPN, we *strongly* recommend the following precautions:

1. Decide which computer you want to host the VPN server. Create the following user account on that computer.
2. Create a new standard user account. This account is your *VPN user account*. FileBrowser will use this account to log onto to the VPN.
 - Do not grant Administrator privileges to this user account!
 - Do not grant access to files and folders to this user account! The VPN user does not need to access folders on your home computer because this user account is only used to create the VPN connection.
 - Assign a strong password to your VPN user account. Use a password that contains a mix of upper- and lower-case characters, numbers and symbols.
3. Turn off (or disable) the guest account on all computers that you intend to to access remotely.

Install a VPN server

If you are connecting to your home network, you must set up a VPN server. The VPN server can run on any PC or Mac on your network, but the computer you choose is effectively the gateway to your home network. This computer must always be turned on if you want to access your network while you are away from home.

- On Windows computers, there is a built-in VPN inside the Professional editions of Windows XP, Vista, 7 and 8. We provide step-by-step instructions for setting up a VPN later in this guide, and also provide a guide on our support web site.
- On a Mac, only a Mac OSX Server has a built-in VPN. Third-party VPN server products are available, but we cannot recommend any of these. Some users have reported success using the iVPN and the VPNActivator products, for example.

You can also find detailed, step-by-step VPN setup guides (with screenshots) on the Stratospherix web site: http://www.stratospherix.com/support/cfwin_bsvpn.php. You may wish to follow those online instructions rather than those below to install and configure the VPN Server.

Windows Vista, 7 and 8

This section describes how to configure the built-in VPN server in Windows 7, 8 and Vista (Professional and Ultimate editions).

1. Decide which computer you want to host the VPN server. Perform the following steps on that computer.
2. From the Control Panel, open the Network and Sharing Center applet.
3. When the applet starts, click 'Change adapter settings' in the left-hand pane.
4. In the Network Connections screen, press the Alt key to display the menu bar.

5. Select 'New Incoming Connection' in the File menu.
6. In the 'Who may connect' screen, you specify which users can connect to the VPN host server. Add the VPN user that you created previously. Then click Next.
7. In the 'How will people connect?' screen, select the 'Through the Internet' check box. Then click Next.
8. In the 'Networking software' screen:
 - a. Select the 'File and Printer Sharing for Microsoft Networks' check box.
 - b. Select the 'Internet Protocol Version 4 (TCP/IPv4)' check box and click the Properties button.
9. In the Incoming IP Properties dialog:
 - a. Select the 'Allow callers to access my local network' check box.
 - b. In the 'IP address assignment' section, select the 'Assign IP addresses automatically using DHCP' option.
 - c. Click OK to close the dialog and return to 'Networking software' screen.
10. Click Allow Access to create the connection.

The Network Connections screen now includes a new 'Incoming Connections' item.

Configure your router to forward Port 1723 traffic

You now need to configure your router or firewall to forward all the VPN network data to your new VPN server.

1. Discover the IP address of the VPN server. Our support page shows how to find the IP address for Windows 7:
http://www.stratospherix.com/support/interactive_troubleshooter/win7-name_res1-2.php shows how to find the IP address for Windows 7.
2. Browse to your router's web page. Then go to the Port Forwarding page.
 - On some routers, this page may be called Firewall Rules or Inbound Services.
 - Also some routers have two Port Forwarding pages, one under Basic Settings and one under Advanced Settings. You will probably need the page under Advanced Settings.
3. Add a new port forwarding rule to send VPN traffic (sometimes called PPTP or GRE) on TCP port 1723 to your VPN server's IP address.

This rule instructs your router to automatically forward data from FileBrowser to the correct computer on your home or office network. (VPN data always uses TCP port 1723 on your router.)

I can't see the VPN service

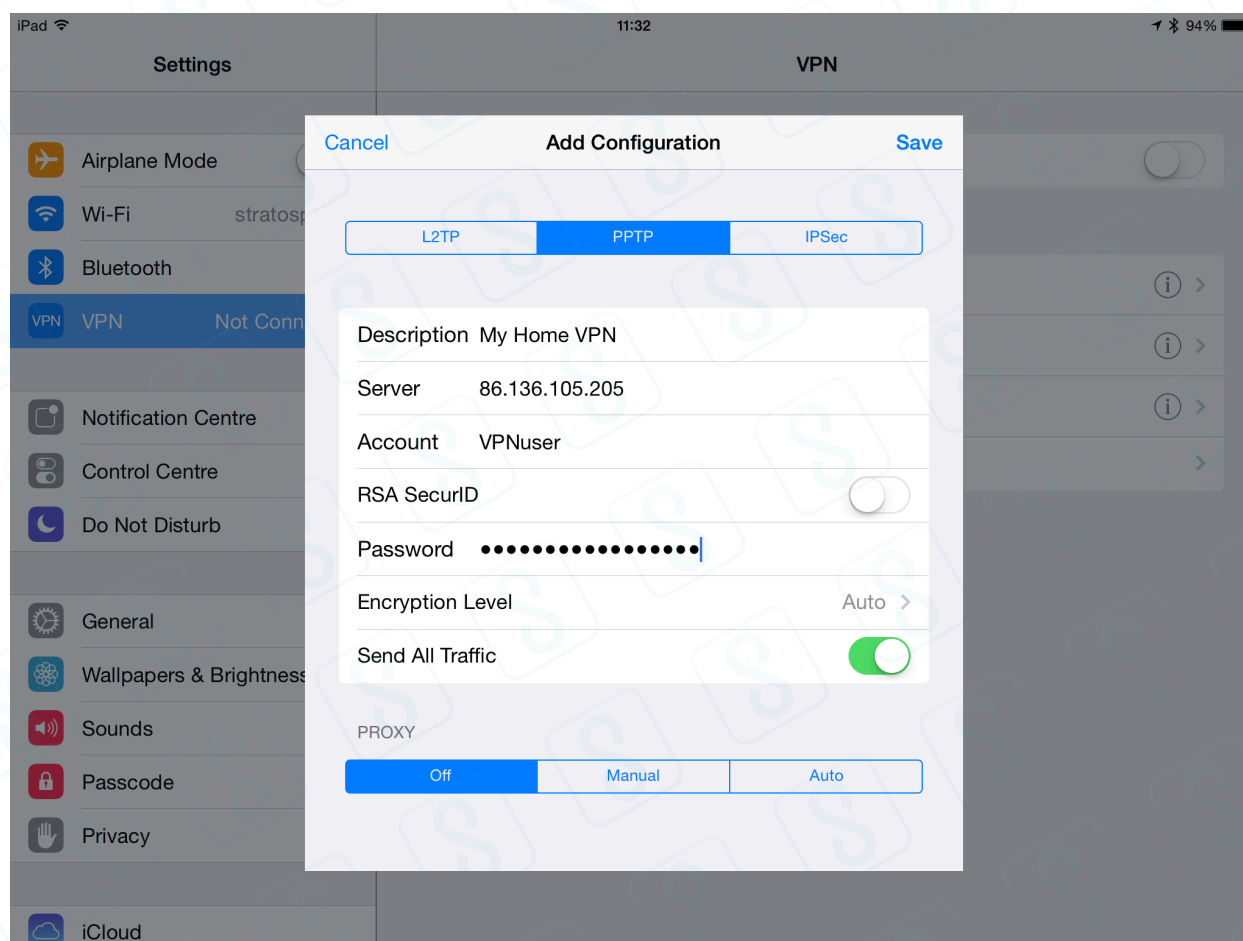
Many routers show a list of common applications, games and services that are eligible for port forwarding. If the VPN service is not included in this predefined list, you will need to create a new service. This is a simple task. [Learn more about creating a new VPN service.](#)

Add a new VPN configuration on your iPad or iPhone

Now you need to add a new VPN configuration to your iPad or iPhone. This configuration uses the VPN server that you installed previously. If you already did this when following our online guide at http://www.stratospherix.com/support/cfwin_bsvpn.php, you may skip this step.

Follow these steps:

1. On your iPad or iPhone, tap **Settings** > **General** > **VPN**.
2. Tap **Add VPN Configuration**.
3. In the Add Configuration screen, tap **PPTP** at the top of the screen.
Note: PPTP is a VPN protocol. The VPN protocol on your iPad or iPhone must be the same as the protocol on your VPN server. If necessary, refer to the VPN instructions on your server to ensure it is configured correctly and runs reliably.
4. In the **Description** field, enter an easy-to-recognize name for your home VPN (for example, 'My Home VPN').
5. In the **Server** field, enter your router's *public* IP address. [What if my router's IP address changes?](#) Alternatively, enter the Dynamic DNS name provided by web sites such no-ip.org. For example, a Dynamic DNS server name my look like this 'johnsmith.no-ip.org'. [Learn more about Dynamic DNS.](#)
6. In the **Account** field, enter the name of the VPN user that you specified in [Create a VPN user account](#).
7. Set **RSA SecurID** field to OFF.
8. In the **Password** field, enter the password for the VPN user account.
9. Set **Send All Traffic** to ON.
10. Set **Proxy** to OFF.
11. Tap **Save** to add the new VPN configuration to the **Choose a Configuration** list in the VPN settings screen.
Note: The check mark next to the new VPN configuration shows that your iPad or iPhone will use this particular VPN configuration when you connect to the VPN. (Some customers may need two separate VPN configurations for connecting to either their home VPN or office VPN.)



Settings screen: Example VPN Configuration

Switch on the VPN on your iPad or iPhone

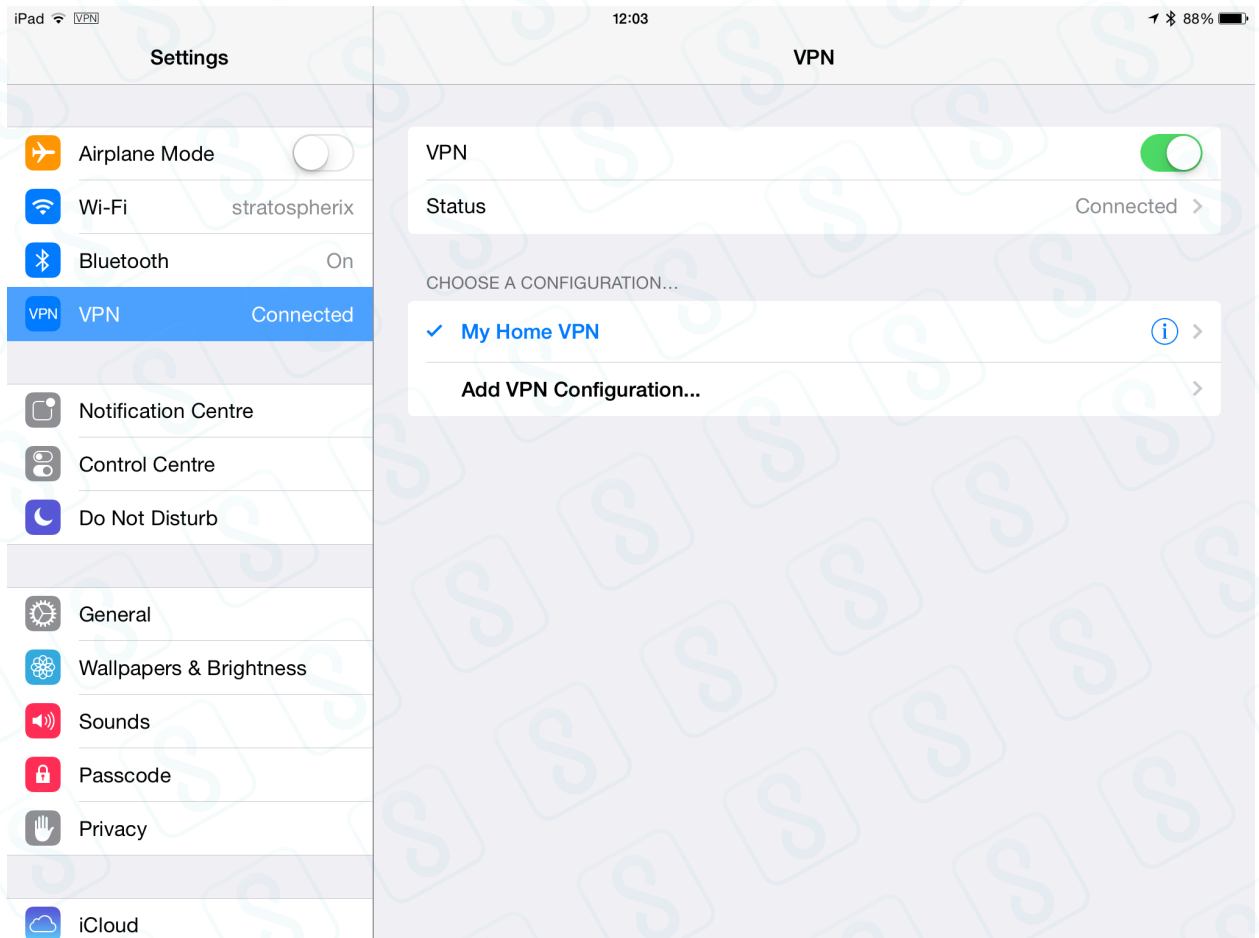
Now you have added a new VPN configuration so your iPad or iPhone can connect to your home VPN server. But you still need to switch on the VPN each time you want to access your home network remotely.

Switching on the VPN activates the VPN configuration that you set up previously. In turn, this connects your iPad or iPhone to your home VPN server. And this connection allows FileBrowser to access any computers on your home network.

When you are away from home, follow these steps each time you want to access your home computers using FileBrowser:

1. On your iPad or iPhone, tap **Settings**.
2. Set **VPN** to **ON**.

A 'VPN Connecting' message appears. Finally, a 'Connected' message displays.



Settings screen: VPN set to ON

3. When you are successfully connected to the VPN, launch FileBrowser.

Test the VPN connection over the Internet

Now you need to confirm that your home VPN is working correctly:

1. Turn *off* WiFi on your iPad or iPhone. This forces it to use the 3G network.
Tap **Wi-Fi** in the **Settings** screen. Then set **Wi-Fi** to OFF.
(If your device doesn't have 3G, you can test the VPN by joining another WiFi network instead.)
2. Switch on the VPN on your iPad or iPhone.
Tap **Settings**. Then set **VPN** to ON.
3. Launch FileBrowser and try to connect to a home computer that you added previously to the Locations list.
See [Add home computers to FileBrowser](#).
4. If FileBrowser cannot connect, see [My VPN still doesn't work!](#)

What happens if the IP address changes on my Internet router?

Unfortunately, this is quite likely. Unless you pay your Internet Service Provider for a fixed IP address, your router's public IP address will change periodically. When this happens you will need to update the VPN settings on your iPad or iPhone with the new public IP address of your router.

You can use a Dynamic DNS service to fix this problem. Dynamic DNS associates a fixed computer name with a dynamic (changeable) IP address. You can then update the your iPad or iPhone VPN settings to use the router's *name* instead of IP address. [Learn more about setting up Dynamic DNS.](#)

Note: Some routers automatically support Dynamic DNS. If yours doesn't, your VPN server computer will need to run some client software provided by the Dynamic DNS service provider that will keep your DDNS name up to date with the public IP address of your Internet router.

[Learn more about IP addresses.](#)

[Learn more about Dynamic DNS.](#)

What happens if the IP address changes on my VPN server?

Your home router is usually configured to be a DHCP server (DHCP is a common network term that stands for Dynamic Host Configuration Protocol). A DHCP server allocates IP addresses to each computer on the network.

When computers on your network are switched off and on again, they may not always be given the same IP address when they restart.

If this happens to your VPN server, you must update the Port Forwarding rule on your router to use the target computer's new IP address. See step 3 in [Configure your router to forward Port 1723 traffic.](#)

You can avoid this problem by using the DHCP IP Address Reservation feature of your router. [Learn more about DHCP IP Address Reservation](#)

My VPN still doesn't work!

If you still cannot connect remotely to computers on your network, check the following:

1. Can you make a local connection to the target computer? That is, can you connect FileBrowser over your home WiFi?
2. If you cannot connect over your home WiFi, you will not be able to connect remotely. You must fix your local connections before attempting a remote connection. For instructions on setting up local connections, see our [Getting Started guides.](#)
3. Is your router forwarding Port 1723 traffic to the IP address of the computer hosting your VPN server?
4. On your iPad or iPhone, check the VPN settings. Verify that the Server field is set to the public IP

address or public DNS name of your router.

[Learn more about IP addresses.](#)

[Learn more about Dynamic DNS.](#)

5. Does your firewall permit connections to TCP Port 1723 on the computer hosting your VPN server? (Sometimes this protocol is called protocol GRE or 47.)
6. If your computer's firewall has blocked this port, you will be unable to connect remotely to the VPN server on your home network. To test whether the port is blocked, you can temporarily disable your firewall. If you *can* connect while the firewall is disabled, you will need to change the scope of your firewall to allow VPN connections through TCP Port 1723 when you re-enable the firewall.

Important! Don't leave your firewall disabled for longer than necessary for this test!

7. If FileBrowser cannot connect to computers in the Locations list, you may need to edit the Address details for these computers in FileBrowser.
Some VPN solutions do not allow *machine identification* packets. If you previously identified computers in the Locations list by name (or name and domain suffix, for example, iMacOne.unipraxis.com), you may need to identify them using their IP address instead.

Port forwarding

With this method, you effectively open a 'hole' in your firewall for FileBrowser. The firewall then allows FileBrowser to connect from the Internet to a specific computer on your network.

[About port forwarding](#)

[How do I set up port forwarding?](#)

[Create an External Access user account](#)

[Choose a port number that is not blocked](#)

[Configure your router to forward SMB traffic on TCP port 445](#)

[Add your router to FileBrowser](#)

[Port forwarding risks](#)

[What happens if IP addresses change?](#)

[Port forwarding still doesn't work!](#)

[Learn more about technical issues.](#)

About Port forwarding

Port forwarding opens a hole in your firewall for specific Internet traffic. It enables FileBrowser to remotely access specific computers on your network.

To use port forwarding requires some basic knowledge about ports. [Learn about ports](#) or [learn about port forwarding](#).

Port forwarding is less secure than using a VPN and we strongly encourage users to use a VPN if possible. Before you proceed to set up port forwarding you **must** ensure you understand the risks. [Learn more about port forwarding risks.](#)

How do I set up port forwarding?

Before you start you need to know if your Internet router supports port translation ([learn about port translation](#)). If it does, the following steps are required. Each step is described fully in the following sections.

1. Create an External Access user on the target computer.
FileBrowser will use this account to connect to the target computer.
2. Choose a port number that is not blocked.
3. Configure your router to forward FileBrowser messages to port 445 on your target computer.
4. Add your router to the Locations list in FileBrowser.

If your Internet router does **not** support port translation you must use the following steps. Please note that this method may make your network more likely to attack from unauthorised users and will

only work if your ISP does not block TCP port 445 (you can use canyouseeme.org to check this).

1. Create an External Access user on the target computer.
FileBrowser will use this account to connect to the target computer.
2. Configure your router to forward FileBrowser messages to port 445 on your target computer.
3. Add your router to the Locations list in FileBrowser.

Create an External Access user account

If you use port forwarding, you must severely restrict remote access to your files on the shared computer. We therefore *strongly* recommend the following precautions:

1. Decide which computer you want to access remotely. This is your *target computer*. Create the following user account on this computer.
2. Create a new standard user account. This account is your *External Access user account*. FileBrowser will use this account to connect to the target computer when you're away from home or out of the office.
 - Do not grant Administrator privileges to this user account!
 - Assign a strong password to your External Access user account. Use a password that contains a mix of upper- and lower-case characters, numbers and symbols.
3. Set up Sharing permissions for your folders on the target folder. In particular, restrict sharing to the new External Access user account. That is, only the External Access user can remotely access your folders. You may also wish to only configure Read-Only access to your files for additional security.
4. Turn off (or disable) the guest account on the target computer.

Choose a port number that is not blocked by your ISP

To avoid inadvertently selecting a port number that is used for another specific purpose, select a port number greater than 10000. Refer to this page for more information:

http://en.wikipedia.org/wiki/TCP_port_numbers. In this guide we use port 20445 as an example, though you can choose another port if you prefer.

Configure your router to forward FileBrowser messages to TCP port 445

Note: With a single port-forward rule you can only configure your router or firewall in this way to connect to one computer on your network. For example, you cannot access your desktop computer and a NAS device at the same time. If your router supports 'Port Translation' you can use this to configure a port-forward rule for each network computer that you wish to access. [Learn more about port translation](#)

Each computer or device on your network has its own IP address. You will need these IP addresses during the setup.

Follow these steps:

1. Discover the IP address of your target computer. [How do I find my computer's IP address?](#)
2. Browse to your router's web page. Then go to the Port Forwarding page.
 - On some routers, this page may be called Firewall Rules or Inbound Services.
 - Also some routers have two Port Forwarding pages, one under Basic Settings and one under Advanced Settings. You will probably need the page under Advanced Settings.
3. **If your router supports port translation** - Add a new port translation rule that forwards incoming data on port 20445 to TCP port 445 on your target computer.
4. **If your router does NOT support port translation** - Add a new port forwarding rule to send SMB traffic on TCP port 445 to your target computer.

This rule instructs your router to automatically forward data from FileBrowser to the target computer on your home or office network. It ensures that your router always uses the correct port to connect to the target computer, regardless of which port FileBrowser used to connect to the router.

I can't see the SMB service

Many routers show a list of common applications, games and services that are eligible for port forwarding. If the SMB service is not included in this predefined list, you will need to create a new SMB service. This is a simple task. [Learn more about creating a new SMB service.](#)

The simplest way to test the port forward rule is to browse to a web page such as [canyouseeme.org](#) from any computer on your home network. You can then enter port number 20445 to check if it is blocked, and if so, re-configure the port forward rule to try another port number.

Add your router to FileBrowser

Now add your *router* to the Locations list in FileBrowser. Do *not* add the target computer that you want to access when you are out of the office or away from home!

Follow these steps:

1. Launch FileBrowser and go to the Locations page.
2. Tap the '+' button in the FileBrowser Locations page.
3. In the **New Machine** screen, specify the machine type (typically PC or Mac).
4. In the **Address** field, enter your router's *public* IP address or Dynamic DNS name.
This public IP address is your router's address on the Internet. When a web server sends Internet traffic to a computer on your network, it routes the traffic via this public IP address.

Important! You must enter your router's **public** IP address. Do not enter the router's private or internal IP address. [Learn more about IP addresses.](#)

How do I find my router's public IP address?

You can typically find your router's public IP address on the status page of your router or firewall. For you may find it on your router's Broadband or Internet Connection page. Alternatively, browse to a web site such as www.whatismyip.com or www.tracemypip.org. Such sites automatically show your router's public IP address.

5. This step applies only if you are using your router's port translation feature.

Important! you must configure FileBrowser to use the chosen port number for this connection. To do this, expand the 'Advanced Settings' section and set the 'SMB Port Number' to your chosen port (20445 in our example above).

6. Tap **Save** to save the new machine details and return to the Locations page.

Port forwarding risks

There are two problems with port forwarding:

- Unauthorized users or malcontents may get access to your network.

After you open a hole in your firewall, anyone on the Internet can potentially use it. Of course, you can set passwords and user restrictions on your file shares to protect them. But suppose you forget to restrict user access? Suppose a determined hacker runs a program that tries all password combinations? Suppose someone discovers a security vulnerability in Windows and exploits it to gain access to your private data?

- Wireless file transfers are not encrypted and are vulnerable to man-in-the-middle (MITM) attacks.

Any data exchanged between your iPad or iPhone and your own network is *not* encrypted (apart from usernames and passwords). So if you use an iPad to view files stored on your network, anyone with access to network traffic can read your files as they transfer. (See that guy in the coffee shop hunched over his laptop? He could be secretly running a WiFi sniffer.)

To avoid these problems, you can instead use a Virtual Private Network (VPN). A VPN is an encrypted link from your iPhone or iPad, through your firewall, to your home or office network. It allows you to connect to the network exactly as if you were connecting over the WiFi at home or in the office. VPN setup was described previously in this guide.

What happens if IP addresses change?

Unfortunately, this is quite likely. IP address changes can affect both your router and the computer that you want to access using FileBrowser.

What if the IP address changes on a home computer?

Your router or firewall allocates a local IP address to each computer on the network, but sometimes these addresses can change.

If this happens, you must update the Port Forwarding rule on your router to use the target computer's new IP address. See step 3 in [Configure your router to forward SMB traffic on TCP port 445](#).

Alternatively, update the Port Forwarding rule to use the computer's name (some routers allow you to do this). This ensures that the rule is always valid, even if the IP address changes again.

Another way to avoid this problem is to use your router's DHCP IP address reservation feature. [Learn more about DHCP IP Address Reservation](#)

What if the public IP address changes on my router?

Unless your Internet Service Provider (ISP) has given you a fixed IP address, it may occasionally assign a new IP address to your router or firewall (even if you never turn them off).

If this happens, you must update the FileBrowser settings to use the new router IP address. See step 4 in [Add your router to FileBrowser](#).

Alternatively, you can use a Dynamic DNS service to fix this problem. Dynamic DNS associates a fixed computer name with a dynamic (changeable) IP address. You can then update the FileBrowser settings to use the router's *name*. [Learn more about setting up Dynamic DNS](#).

Port forwarding still doesn't work!

If you still cannot connect remotely to your target computer, check the following:

1. Can you make a local connection to the target computer? That is, can you connect FileBrowser over your home or office WiFi?

If you cannot connect over your home or office WiFi, you will not be able to connect remotely. You must fix your local connection before attempting a remote connection. For instructions on setting up local connections, see our [Getting Started guides](#).

2. Does the Port Forwarding rule for SMB on your router point to the correct (local) IP address of the target computer or NAS device.
3. Does your computer firewall permit connections to TCP Port 445?

If your firewall has blocked this port, you will be unable to connect remotely to the target computer on your home or office network. To test whether the port is blocked, you can temporarily disable your firewall. If you *can* connect while the firewall is disabled, you will need to change the scope of your firewall to allow SMB connections through TCP Port 445 when you re-enable the firewall. [Learn more about changing the firewall scope](#).

Important! Don't leave your firewall disabled for longer than necessary for this test!

4. If you are using port translation, did you enter the same port number in the FileBrowser 'SMB Port Number' field as you used in the port translation rule?
5. Is FileBrowser using your router's *public* IP address or *public* DNS name? To test this:
 - a. In the Settings screen on your iPad or iPhone, turn on WiFi and connect to your home or office network.
 - b. Launch FileBrowser. Then go to the Locations screen and connect to your target computer.
 - c. If you can successfully connect, turn off WiFi on your iPad or iPhone.
 - d. Can you still connect to the target computer using 3G? If you can successfully connect over 3G, FileBrowser is correctly configured to use your router's public IP address.
6. Some ISPs do not allow SMB file sharing network traffic through to your router. These issues mainly affect US customers.

If you suspect that either case applies to you, you must **Either** set up a Virtual Private Network (VPN) to allow FileBrowser remote access to your network ([Learn more about VPNs](#)) **Or** use 'Port Translation' so that FileBrowser is able to use a different TCP Port number than 445. [Learn more about port translation](#).

Learn More

[About IP addresses](#)

[About ports](#)

[About port forwarding](#)

[How do I set up a Dynamic DNS service?](#)

[How do I prevent my computer's IP Address from changing?](#)

[About port translation](#)

[How do I create a new VPN service?](#)

[How do I create a new SMB service?](#)

[How do I change the scope of my firewall?](#)

About IP addresses

In simple terms, imagine that your network is like a hotel. Each computer or device on the network is like a hotel room. Just as each hotel room has a unique name or room number (eg, Room 125), so each computer or device has its own name or IP address (eg, 'Spencer's Laptop' or 192.168.1.83).

However, your router has two IP addresses: a private address and a public address. Why? Because your router is like a combination of the hotel lobby and the hotel main entrance. Hotel guests understand that the lobby is an internal location ("meet me in the lobby in five"). But the hotel main entrance is the external location that taxi drivers understand ("take me to the Metropolitan").

Your router's *private* IP address (sometimes called its *gateway* address) is equivalent to the hotel lobby. It usually takes the same subnet form as the addresses for other computers on your network (for example, 192.168.1.254 or 192.168.1.1). Computers on your network connect to the router using this internal address. The router then routes the computers data out onto the Internet.

Your router's *public* IP address (sometimes called its *broadband network address*) is equivalent to the hotel main entrance. It is used by web servers to send Internet traffic, via your router, to computers on your network. The number combination in this public IP address will be very different from the IP addresses of computers on your network (for example, 86.136.105.206).

How do I find my computer's IP address?

Windows computers: Run the Command Prompt applet (find this in the Accessories folder). Type the command 'ipconfig'. Then look for the IP or IPv4 address in the output; this is your computer's IP address and it will usually start with 192.168.x.x or 10.x.x.x.

Apple Macs: Click the Apple logo. Then select System Preferences > Network. The IP address for your Mac is shown in the next window.

NAS devices: The IP address is typically listed on the device's Status or Configuration web page.

About network ports

A port serves as the connection point when a computer communicates with another computer or device. A computer's IP address allows messages to be sent to the computer over the network, but computers receive many different types of message. For example when you use a web browser to view a web page, your computer requests the contents of the web page and this information is sent to your computer using its IP address. If an email arrives at the same time as a web page is loading, the computer is able to tell the difference between the email data and the web page data. This is achieved using **ports**.

A 'port' is just a number, but it is also a label that identifies the kind of data that a message contains. In our hotel room example, ports can be considered as a series of in-trays on the desk, where messages are sorted as they arrive. So for example, if our hotel room is being used as the headquarters for an election campaign, many different types of correspondence will arrive and depending on the type of message (campaign contribution, request from a newspaper for an interview or complaint from a constituent) these might be sorted into different in-boxes (finance, PR, garbage) so that they can be handled by the appropriate person.

For FileBrowser, messages sent to remote computers must be identifiable as file browsing requests and in this case the relevant port number is 445. That is, unless the message is labelled with the port number 445, the remote computer will not recognize the request as a file browsing request and will ignore it.

About port forwarding

Because the port number in every Internet message identifies the kind of information contained within the message, your Internet router can use this information to only allow certain type of message through its built in firewall. In fact, Internet routers normally only allow information through from the Internet to your private home network if the message is a direct response to a request from a computer on your network - such as a request to a web server for a web page, or a request from your email program for any new emails.

This means that your router will routinely ignore all messages sent by FileBrowser when you connect to your network remotely. Unless you configure the router otherwise!

In our hotel example, the secretary picks up the mail from the front desk and discards any complaints before they can be sorted into the in-trays because the campaign team regards such correspondence as a waste of time.

But what if the campaign team needs to find out what constituents are complaining about? One solution would be to install some interns in a room down the corridor. The secretary could then pass the complaints to the interns for them to read, instead of simply throwing them away.

Port forwarding performs a similar task. Instead of ignoring data, the router allows in specific types

of message and sends them to a specific computer's network (IP) address.

It is important to realise that there are risks associated with port forwarding. [Learn more about port forwarding risks.](#)

Some Internet Service Providers (ISPs) block Port 445

One complication is that many ISPs and 3G mobile providers block any messages that use port 445 (the port that FileBrowser must use to access the remote computer).

In our example, this would be similar to the mailman discarding any letters with 'Complaint' on the envelope before they are delivered to the hotel. This is because the mailman knows that the campaign team is not interested in complaints.

One way to get around this problem would be to write 'Campaign contribution' on the envelope so that the complaint would be delivered. When the secretary opens the mail to sort it, its true nature would become apparent and it would be handled accordingly.

In the same way, messages from FileBrowser can start out labelled with a port number that the ISP does **not** block so that the message reaches your Internet router. As long as *something* changes the port to the correct one (445) before the message reaches the remote computer, the remote computer will receive the message and answer with the required data.

In practice, the *something* that does this is your Internet router, using port translation. [Learn more about port translation.](#)

About port translation

Port translation is a feature of routers that is used with port forwarding. With port translation, instead of forwarding network data to a specified computer or NAS using the same port number as when the data arrived at the router, the router is able to change the port number when it passes on the data.

Some routers label the port numbers as 'Public Port' and 'Private port'. The Public Port is the port number that the router listens for on its public IP address, and the Private Port will be the port number used by your local network computers. For FileBrowser, which uses the SMB network protocol, the Private Port will be TCP 445.

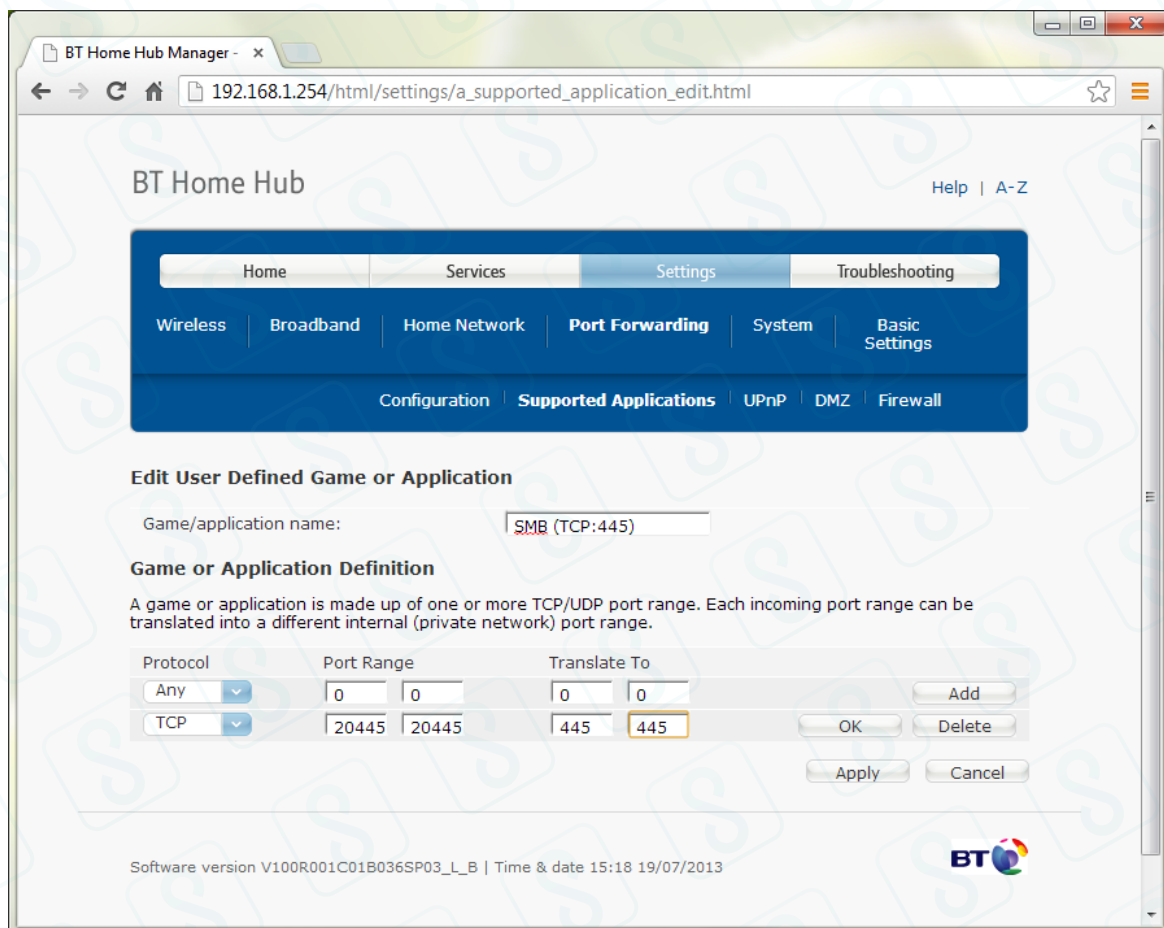
Note: Computers use the TCP protocol (or 'language') to communicate with each other over the Internet. Using TCP is like sending a Fedex package that the recipient must sign for when the package arrives. FileBrowser always uses TCP to deliver its messages.

Port translation can be used to work around the restriction imposed by some ISPs who block TCP Port 445. It can also be used to provide access via Port Forwarding to more than one computer on your home network.

As an example, let's assume that our network computer is using IP address 192.168.1.5 and our ISP blocks TCP port 445. We could configure FileBrowser and our router as follows to use TCP Port 20445 for the Internet section of the connection to our network computer.

In the router's port forwarding rule that we have created ([Learn more about creating a SMB service](#)), use the following settings:

- **Public UDP Port:** <Leave blank>
- **Public TCP Port:** 20445
- **Private UDP Port:** <Leave blank>
- **Private TCP Port:** 445



Example: BT Home Hub, Port Forwarding, Supported Applications screen. This screen shows a rule being set up to translate FileBrowser data arriving on TCP port 20445 to TCP port 445.

In FileBrowser's Advanced Settings section of the configuration for this connection:

- Change the SMB Port Number field from 445 to 20445.

How do I set up a Dynamic DNS service?

You must register with a Dynamic DNS provider. The provider tracks your router's changing IP address and assigns a permanent network name (also called a domain name) to your router. You can then use this name to identify the router instead of an IP address.

When you identify the router in the FileBrowser's New Machine screen, you can enter the network name supplied by your Dynamic DNS provider in the Address field.

Some routers have a built-in Dynamic DNS service that you can use. If not, use the free service provider www.no-ip.com. See their web site for simple instructions. Permanent network names typically take this format:

MyDDNSRouterName.no-ip.org

Note: Dynamic DNS providers typically require that you run a small monitoring program (a 'Dynamic Update Client') continuously to track IP address changes. This will need to run on one of your home computers (such as your VPN server) if your router doesn't support Dynamic DNS.

How do I prevent my computer's IP Address from changing?

The IP address of a network computer may change periodically or when it is restarted. This is because the DHCP server allocates IP addresses to the network computers as they request them, similar to an airline check-in allocating seat numbers.

Most routers have an IP Address reservation feature that allows them to always give the same IP address to a specific network computer or device. The Settings for this feature can generally be found on the same router configuration page as that showing which devices are attached and the IP addresses assigned to them. This is usually in the DHCP section.

How do I create a new VPN service?

Most routers include an advanced Port Forwarding feature that allows you to do add new applications, games and services. The details that you must enter will vary from router to router, but typically include fields such as these:

- **Name:** We recommend that you enter 'VPN'.
- **Protocol:** This must be 'TCP'.
- **Port range to:** Enter '1723 to 1723'.
- **Translate to:** Enter '1723 to 1723'.
- **Send to or Devices:** Enter the name or IP address of the computer hosting the VPN server on your home network. FileBrowser connects to the VPN server when you're away from home or out of the office.

How do I create a new SMB service?

Most routers include an advanced Port Forwarding feature that allows you to do add new applications, games and services. The details that you must enter will vary from router to router, but typically include fields such as these:

- **Name:** We recommend that you enter 'SMB (TCP:445)'.
- **Protocol:** This must be 'TCP'.
- **Port range to:** Enter '445 to 445'.
- **Translate to:** Enter '445 to 445'.
- **Send to or Devices:** Enter the name or IP address of the target computer. This is the network computer you want FileBrowser to access when you are away from home or out of the office.

BT Home Hub Manager - x

192.168.1.254/html/settings/a_supported_application_edit.html

BT Home Hub

Help | A-Z

Home Services Settings Troubleshooting

Wireless Broadband Home Network Port Forwarding System Basic Settings

Configuration Supported Applications UPnP DMZ Firewall

Edit User Defined Game or Application

Game/application name: SMB (TCP:445)

Game or Application Definition

A game or application is made up of one or more TCP/UDP port range. Each incoming port range can be translated into a different internal (private network) port range.

Protocol	Port Range	Translate To
Any	0 0	0 0
TCP	445 445	445 445

Add OK Delete Apply Cancel

Software version V100R001C01B036SP03_L_B | Time & date 15:18 19/07/2013

BT

Example: BT Home Hub, Port Forwarding, Supported Applications screen. This screen shows an SMB rule being set up to forward FileBrowser data. You then assign this new rule to the target computer in the Port Forwarding, Configuration page.

How do I change the scope of my computer's firewall?

(Applies to Port Forwarding only)

On Windows computers, the firewall scope may be set to block connections from the Internet to the target computer. To reconfigure the firewall to accept connections from the Internet, follow these steps.

On Windows 7 computers, follow these steps:

1. In the Control Panel, open the Windows Firewall applet.
2. Click the 'Allow a program or feature through Windows Firewall' link.
 - a. In the next screen, click Change Settings.
 - b. In the Allowed Programs list, find 'File and Printer Sharing' and select the 'Home/Work (Private)' check box.
 - c. Click OK to return to the main Windows Firewall screen.
3. Click the 'Advanced settings' link.
 - a. In the Advanced Security screen, select Inbound Rules in the left-hand pane.
 - b. In the middle pane, find the 'File and Printer Sharing (SMB-In)' rules. There are three rules, differentiated by their Profile. (The Profile column is set to Public, Private and Domain respectively.)
Note that rules are not listed alphabetically in this list.
 - c. Right-click the 'File and Printer Sharing (SMB-In)' rule with a Private Profile and click Properties.
 - d. In the Properties dialog, go to the Scope tab.
 - e. In the Remote IP Address section, select 'Any IP address' and click OK.

On Windows 8 computers, follow these steps:

1. Type 'Firewall' on the Windows tile screen to search for the Firewall Control Panel app.
2. Click the 'Allow an app or Windows feature through Windows Firewall' link.
3. Click Change Settings.
4. Scroll to 'File and Printer Sharing'.
5. Ensure that the option is selected and both Private and Public are selected too.
6. Click OK.

On Windows XP computers, follow these steps:

1. In the Control Panel, open the Windows Firewall applet.
2. Go to the Exceptions tab.
3. Select 'File and Printer Sharing' and click Edit.
4. In the popup dialog, select 'TCP 445' and click Change scope.
5. In the next dialog, select 'Any computer (including those on the Internet)'. Click OK on all open windows.