Accessing CharityMaster data from another location

When all of your computers are on the same Local Area Network (LAN), you can place the "back end" files (including your data and the Word templates) onto one machine or a server and all of the workstations on the network can be "pointed" to these "back end" files. This guide will show you how it is possible to access a CharityMaster database using a workstation that is NOT connected to your LAN.

We recommend that you DO NOT use WiFi to connect your computer with the back end database – even on a LAN in the confines of your office. Wired connections are much more dependable.

Connect to your data over the internet

Consider the situation where your CharityMaster "back end" database is stored on a computer or server in your organization's main office. If the machine on which your data are stored is connected to the internet, you can connect any ***Client*** computer to your database (provided the ***Client*** computer has the CharityMaster "front end" program installed.) Using this approach, up to five ***Client*** computers can access the CharityMaster database at the same time.

To connect CharityMaster to a "back end" database which is not in your location, proceed as follows:

- Set up a VPN (recommended)
- Create a Network Location shortcut on your computer that will allow CharityMaster to find the computer or server where the database is located.
- Using the Network Location, "point" CharityMaster to your database.

Virtual Private Networks

It is possible to establish an internet connection between CharityMaster and your database without using a Virtual Private Network (VPN) but all of your data will be visible to anyone who wants to read it. You should establish the connection using a VPN. A VPN creates a secure "tunnel" between a client device and a Local Area Network (LAN) and, while the packets of your data traverse the open Internet, they are encrypted.

VPNs can be either software based or hardware based:

- Software based VPNs use a service provider to encrypt your data. Your data travels from your computer to the service provider and then to your CharityMaster database (and back again). One of the least expensive (less than $50 US per year) and easiest to use is PrivateInternetAccess.com. Up to five devices can share the VPN (e.g. connect to your database) at the same time.
- A hardware VPN is a virtual private network based on a device that is connected to the LAN in your organization's office. The device will contain a processor, manage authentication, encryption, and other VPN functions, and usually provides a hardware firewall. There are several routers that

include VPN functions or you can configure an “always on” PC on the office LAN to be a VPN server. Hardware VPNs offer several features that software VPNs do not but they are generally more expensive than software VPNs.

Note that when you connect to a VPN, ALL of your communications over the internet are encrypted – not just the communication between a client computer and your CharityMaster database. For this reason alone, you may wish to install a VPN in your organization.

We recommend that you ask an IT specialist to advise you on the best, and least expensive way to set up a VPN.

Setting up a Network Location

You can create shortcuts on your computer to a web resource like a server located in your organization’s office. The process for creating this type of shortcut is named “creating a Network Location.” A Network Location has the following characteristics:

- It is a shortcut to a web location like a web site or a file server.
- It can point to either external resources found on the internet or to resources found in your local area network.
- You need the appropriate credentials to connect to it.
- It doesn’t have a driver letter assigned.

Instructions for Windows computers are in Annex B below. Consult a Mac expert for how to do the equivalent on a Mac computer.

Remote Desktop – peer to peer

Most Windows operating systems allow a ***Client*** computer to take mouse and keyboard control over a computer that has CharityMaster installed (the ***Remote*** computer) while showing you everything that's happening on the ***Remote*** computer’s screen. With Remote Desktop, there is no need to install CharityMaster on the ***Client*** computer since it will be running on the ***Remote*** computer. You can also print CharityMaster reports and Word outputs using any printer connected to the ***Client*** computer. You do not have to buy anything to implement this solution.

To use Windows Remote Desktop you download free software onto any Windows or Mac OS X ***Client*** computer with an internet connection to access a ***Remote*** computer that is running Windows. Microsoft has also developed Remote Desktop ***Client*** apps for iOS and Android devices.

Contact us if you would like to see CharityMaster in operation using this technology. It will take you just a couple of minutes to access CharityMaster installed on a server in our office.

Remote Desktop solutions require the following:

- The ***Remote*** computer running CharityMaster must have the Windows *Professional* operating system. You may have to upgrade the version of Windows that is running on the ***Remote*** computer.
- The ***Remote*** computer must be running 24 / 7 to allow for access at any time. (It cannot be in sleep or hibernate mode.)
- The ***Remote*** computer must have a user account set up with credentials (user name and password) that are known to the person using the ***Client*** computer.)

- The ***Remote*** computer must be connected directly to the internet or be on a Local Area Network (LAN) that is connected to the Internet.
- The free Remote Desktop Client must be downloaded and installed on the ***Client*** computer or device.

An important limitation of Remote Desktop is the fact that only ONE client can connect to the ***Remote*** PC at any one time. This limitation applies to Windows 10 and previous versions of Windows but it does NOT apply to systems running Windows Server.

You can also use Remote Desktop to run applications other than CharityMaster that are installed on the ***Remote*** computer. So if you have purchased the QuickBooks interface module for CharityMaster and QuickBooks is installed on the ***Remote*** computer you can enter your revenue transactions into CharityMaster anywhere in the world and have them automatically entered into QuickBooks.

Instructions for setting up ***Remote*** desktop on a Windows 10 computer running CharityMaster are in Annex A below. Instructions for earlier operating systems are similar.

If you have the Google Chrome browser installed on both the ***Client*** and ***Remote*** computers, you can use the free Chrome Remote Desktop browser extension to accomplish the same thing as Windows Remote desktop for Windows 10.

Security of Remote Desktop solutions

You do not need to have a VPN since the Remote Desktop software has its own built in security.

By default, the only people who can access the ***Remote*** computer are those with an Administrator user account on the ***Remote*** machine. This means that Remote Desktop users can access and change everything on the ***Remote*** computer – not just CharityMaster. We recommend the following:

- Change the Windows 10 settings to allow non-Administrator users to access the Remote machine. (You will have to specifically state which non-Administrator user accounts have access to the Remote Desktop service.)
- Mitigate the risks by having one computer dedicated to running Remote Desktop which has just CharityMaster and Microsoft Word installed.

Also, it is important to note that anyone accessing the ***Remote*** computer can also access any connected network drives that are not secured. If you have a network drive that will (or already does) contain sensitive or private data, protect the drive from access by unauthorized users by configuring the security settings for the folders that are on each network drive.

To protect your data that is moving over the internet, you should configure your ***Remote*** computer to use the highest level of encryption for Remote Desktop communications.

Remote Desktop – Windows Server solution

If your organization has a machine running *Windows Server* in your office, then the server can be set up to allow for multiple users to *simultaneously* access CharityMaster on the server. You will have to buy Remote Desktop Services (RDS) Client Access Licenses (CALS) for each user that will be accessing the server over the internet. (Users can share a single RDS CALS but only one user can use a CALS at a time.)

Windows Servers can be configured to restrict users' access to specific applications (e.g. CharityMaster and

Word) and file folders.

Commercial Remote Desktop services

In addition to Remote Desktop, there are several commercial services that may charge a monthly fee for connecting over the internet. These have the advantage of super-simple setup and, in some cases, the ability to use tablets with any operating system and Mac computers to access a ***Remote*** computer. ***Client*** computers can access *everything* on the ***Remote*** computer but they only allow *one user at a time* to access a single computer.

There are several FREE services but the best is arguably Team Viewer. Team Viewer offers a free license *for non-commercial* use that allows one ***Client*** computer at a time to control a ***Remote*** computer. After you create the free Team Viewer account and add the computer that is running CharityMaster to the list of "trusted" computers, anyone with the Team Viewer account credentials can sign into the Team Viewer account and connect to the remote computer.

Another free service is Remote Utilities which is free for both personal and commercial use. However, it does not run on Mac computers or on tablets. Other commercial (paid) remote desktop services include GoToMyPC (US site) or GoToMyPC (Canadian site) and LogMeIn Pro.

Security of *commercial* Remote Desktop solutions

Keep in mind that commercial Remote Desktop solutions generally allow the ***Client*** computer to access and change *everything* on the ***Remote*** computer – not just CharityMaster. Some commercial services allow you to override this setting. You can also mitigate the risks by having one computer dedicated to running Remote Desktop which has just CharityMaster and Microsoft Word installed.

It is important to note that anyone accessing the ***Remote*** computer can also access any connected network drives that are not secured. If you have a network drive that will (or already does) contain sensitive or private data, protect the drive from unauthorized users by configuring the security settings for the folders that are on each network drive.

Application Hosting

What is application hosting?

Application Hosting is a service provided by a number of companies. A *hosted* application is a software as a service (SaaS) solution that allows users to execute and operate a software application entirely from the cloud on a recurring subscription.

Hosted applications are hosted and powered from the remote cloud computer infrastructure and are accessed globally through the Internet. They provide the same functionality as locally installed software but can be updated more easily.

Application hosting gives you the ability to access and edit all of your data from any location using any device without any requirements other than having a web browser and an active internet connection. This means that, no matter where you are in the world, you will always have quick access to your CharityMaster data. When you use a hosted version of CharityMaster you still have the ability to edit data, run reports, write letters, send e-mails or use any of the normal functions you would typically use in your office.

CharityMaster has partnered with a hosting provider to provide hosting for both CharityMaster and

QuickBooks. CharityMaster's amazing integration with QuickBooks means that every time you enter a transaction into CharityMaster, accurate entries are immediately posted into QuickBooks. You will save lots of time and eliminate most accounting errors. With QuickBooks hosting, your bookkeeper can have immediate access to your data from their office.

See our web site for details.

Benefits of hosting

Any place access

Your staff and volunteers can enter or review data from their homes or offices or from the locations of your events using any device. You can even use your smart phone! All they need is a web browser.

Save money

No need to purchase servers or pay for off-site backup and storage. You're really only adding a small monthly fee to upgrade your IT infrastructure instead of continuing to invest in more hardware and software maintenance.

Save time

- No more time and effort downloading and installing updates. You always have the latest versions.
- With hosted QuickBooks, you minimize the time to send copies of files, documents, listings, etc. to your bookkeeper every month.

Security and data protection

- All of your data is secure. You communicate with the hosting company over a secure connection and all of your data and documents stored on the host servers are backed up daily. Enterprise level security ensures that no one can access your data without your permission.
- Working in the cloud is usually safer and more affordable than what typical not-for-profits can afford since it entails using enterprise resources at monitored and professionally maintained datacenters. Consider whether or not your data would be safe if there were a fire or flood at your location. If it's safely stored in the cloud, it can quickly and easily be retrieved.
- No need to worry about lost or stolen laptops or other hardware.
- Download a copy of all of your data and documents at any time.

Use *any* device

- Desktop and laptop PCs
- Mac computers
- Any tablet or smart phone
- All you need is an internet connection, your favorite browser and the free Citrix receiver software.

Using cloud storage

Some organizations may be tempted to use internet storage services such as Google Drive, OneDrive, DropBox, etc. to store their data. We do not recommend this approach. These services are all file "syncing" services which means that a copy of all of the files that are stored in the cloud are also on your PC. When you make a change to a file on your PC (by entering data in CharityMaster for example), a copy of that file is immediately sent to the cloud storage.

This approach will work only when there is only ONE person connected to your CharityMaster database since every time a change is made to your data the local file will be changed and the file sharing service will

attempt to synchronize the local database file with the database file stored in the “cloud.” If another user is doing the same thing at the same time, data changes will almost certainly be lost.

Annex A – How to set up Remote Desktop access

The following assumes that you have Windows 10 or later installed on both the machine running CharityMaster (the ***Remote*** computer) and the ***Client*** computer. Instructions for earlier Windows versions are similar.

Note that the ***Client*** computer does NOT have to have the CharityMaster program installed. *Any* Windows or Mac computer can access a **Remote** (target) computer that has been set up with Remote Desktop. Microsoft has also developed Remote Desktop ***Client*** apps for iOS and Android devices.

Setting up

Remote (target) PC

In order to be able to use Remote Desktop Connection you'll first have to allow remote access to your ***Remote*** PC (the one running CharityMaster.)

To do this yourself, open **File Explorer**, find **This PC** and right-click to bring up the contextual menu. Now select **Properties** > **Remote Settings** and in the "Remote Desktop" section make sure that the *Allow remote connections to this computer* option is selected and tick the *Allow connections only from computers running Remote Desktop with Network Level Authentication*. Now click Apply and OK.

Before you can connect to your target PC you'll need to know its IP address so that it can be found on your Local Area Network (LAN) network. To do this hold down the Windows key and press R. In the box that appears type *cmd* and press enter. In the terminal windows that appears type *ipconfig* and press enter. You'll see a range of information appear, but the one you want is IPv4 Address. Note this down (it's a few numbers and full stops) and also write down the Default Gateway IP address.

The IPv4 address will allow you to access the PC on a local network, but if you want to access it from a WAN (i.e. if you're at home and want to access the CharityMaster machine in the office) then open up a browser and in the address bar type in "whatismyipaddress" (no spaces or quotes) then make a note of the address.

It's important to note that if you intend to use the internet to connect to the Remote PC on a regular basis, the external Wide Area Network (WAN) IP address is subject to change unless you have paid for a *static* IP address from your internet service provider. To avoid having to rediscover the external IP address every time this happens, subscribe to a dynamic DNS service such as Dyn or no-ip.com, as this gives you a memorable domain name to which you can connect. To ensure that the DNS service that you have subscribed to knows about any changes to your external IP address, you will have to either:

- Set up your router to automatically update any changes to your external IP address. Many routers have built-in support for dynamic DNS, so have a look in your manual and select one of the services supported by your router.
- Download a small program from your DNS service provider that will keep your DNS service provider up to date. This program will be installed on the ***Remote*** computer.

Next, you'll need to make sure the Windows firewall isn't blocking Remote Desktop. You can check this by opening up the Windows Firewall section of the Control Panel and selecting *Allow apps to communicate through Windows Firewall*. Of course, if you are using a different firewall program such as McAfee, the procedure is somewhat different.

Now you'll need to configure your router so that it knows the correct addresses for your computers, and enable the Port Forward setting so that it points at Port 3389. As router settings are different on every router, you can go to a fabulous website dedicated to helping you with this step: https://portforward.com

Client PC

With all of this completed, you should now be able to open the Windows Start Menu, search for Remote Desktop, select "Remote Desktop Connection" then, in the box that appears, type the domain name or IP address and click Connect. Enter your username and password, then you should have full access to the Remote PC.

Alternatively, download and install the Remote Desktop app from the Microsoft Store or the iTunes store. We recommend this approach because this app has more features than the connector that was installed as part of Windows.

Remote Access security

It is essential that you set up a *standard* (non-Administrator) account for each person that is going to remotely access this machine and that each of them are provided with a very strong password. Once you have added a user, you must also add them to the list of Remote Desktop Users as outlined in this article: How to enable and secure remote desktop on Windows.

We strongly recommend that you do *not* use the default security settings for Remote Desktop. After you have implemented the recommended steps to improve security, some users with older machines may not be able to connect to the ***Remote*** computer. They will have to download the latest Remote Desktop connector from Microsoft or the iTunes store.

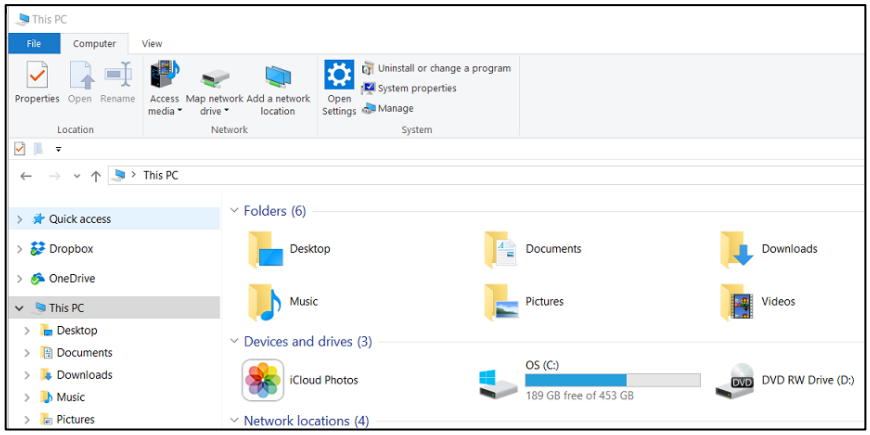
Annex B – Creating a Network Location

Before you start

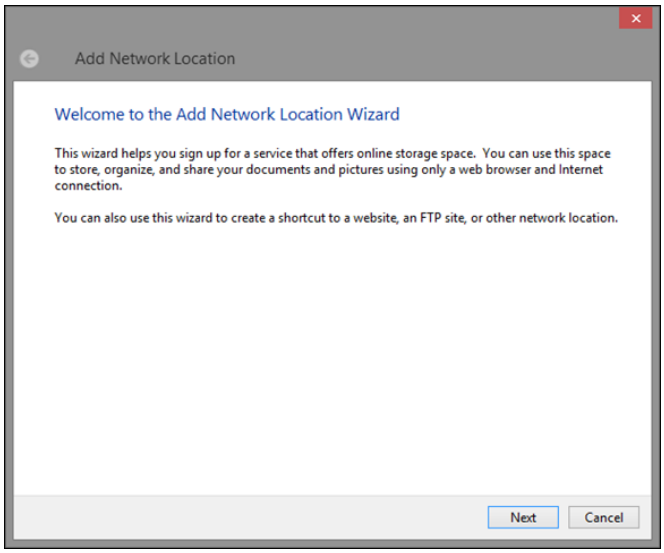
- The folder containing the CharityMaster database on the computer or server you are trying to access must be set to SHARED. All users accessing this folder must have both Read and Write permissions. An excellent article on file and folder sharing is How to set up file sharing on Windows 10. We recommend that you allow sharing only with users who have an account on this computer. That makes it easier to remove sharing from a specific individual.
- The computer or server you are trying to access must be ON and running. If the computer is sleeping, you cannot access that folder.
- You must know the credentials (user name and password) of the folder, computer, or website you are trying to map or connect as a network location.

On the computer running CharityMaster

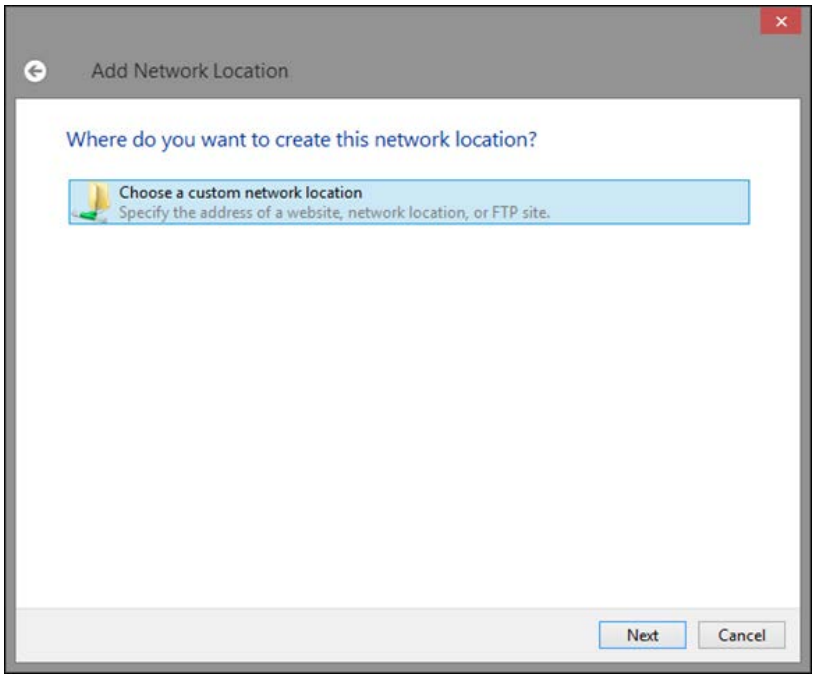
Mapping the address of a website location is done using the "Add Network Location" wizard. In Windows 10 you need to start File Explorer and go to "This PC." Then, expand the Computer tab on the ribbon and click or tap "Add a network location".



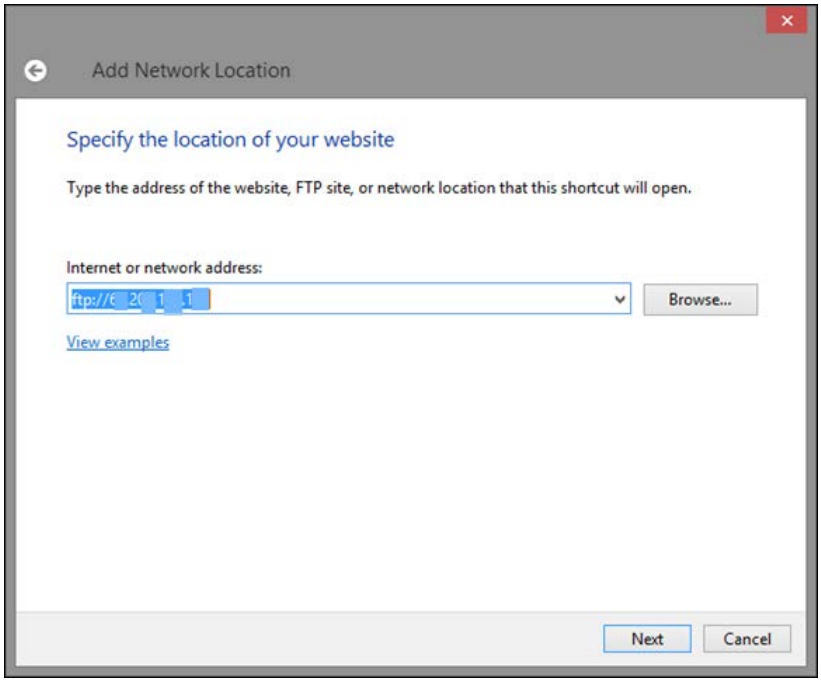
Click on it and the wizard starts. Press "Next".



You are then asked where you want to create this network location and given only one choice. Select “Choose a custom network location” and press “Next”.

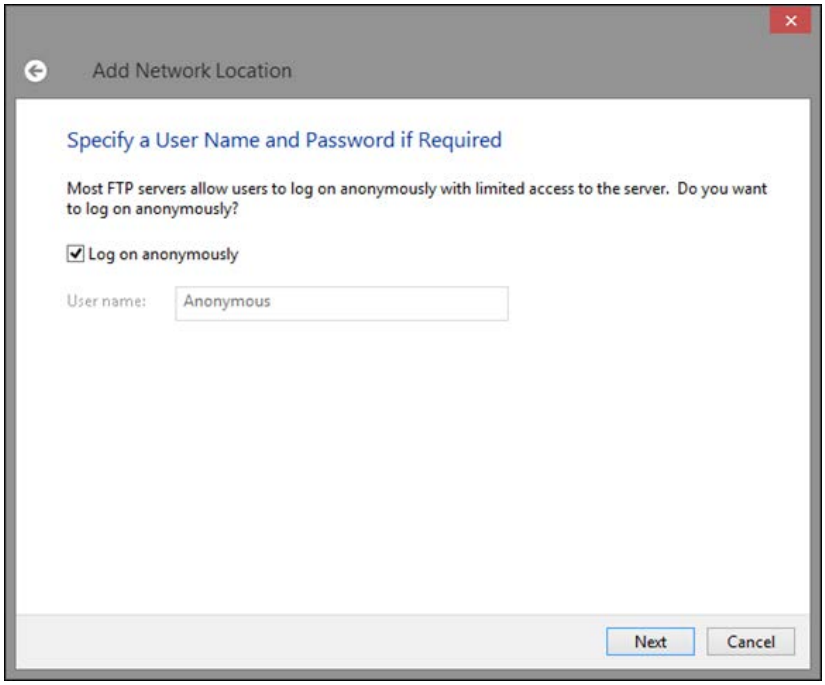


Next you are asked to give the internet address of the web site you want to add. To add a web share, you should type “http://” or “https://” – depending on the protocol used by the web share, followed by the web servers IP address or the web site URL and then “/” followed by the share name. For example: **http://charitymaster.com/sharename** or **https://192.168.1.2/sharename**

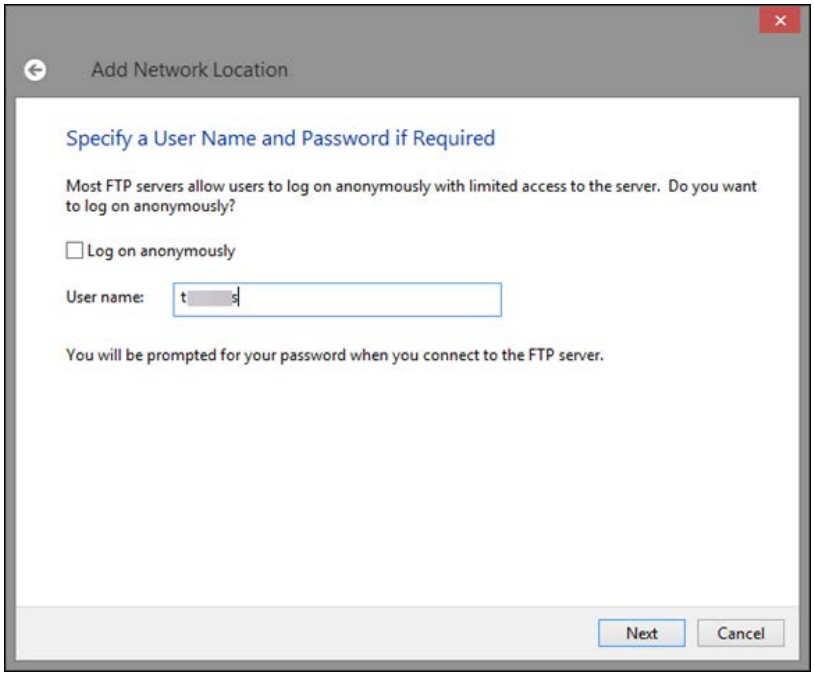


Press “Next”.

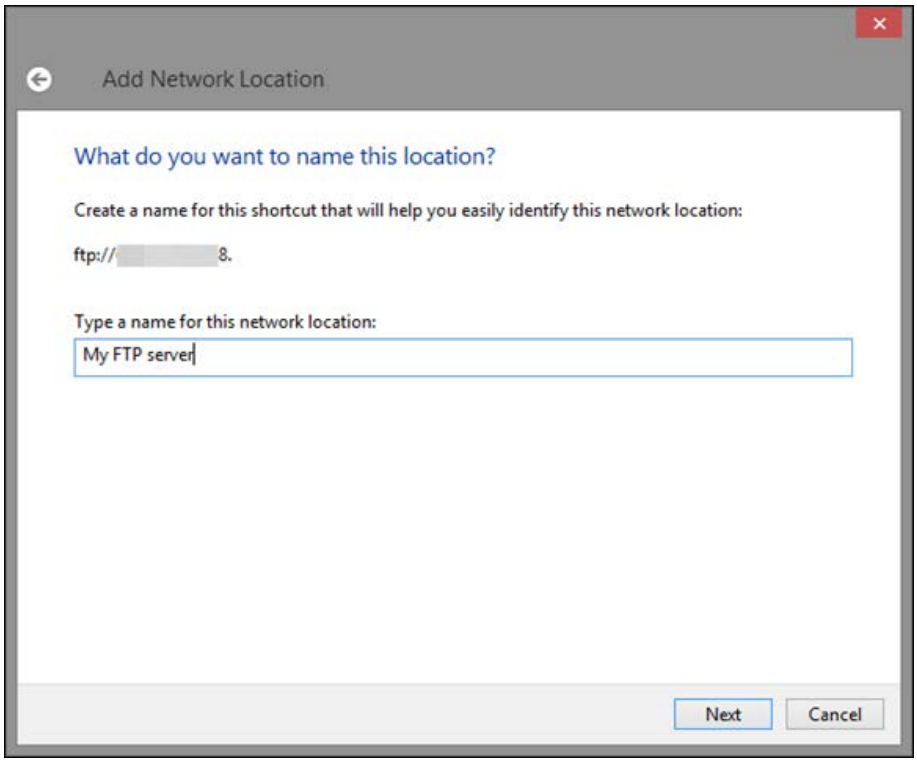
You are asked to enter a user name and password if they are required. If you cannot log in anonymously, clear the box that says “Log on anonymously”. If you can log in anonymously, press “Next” and skip the next step.



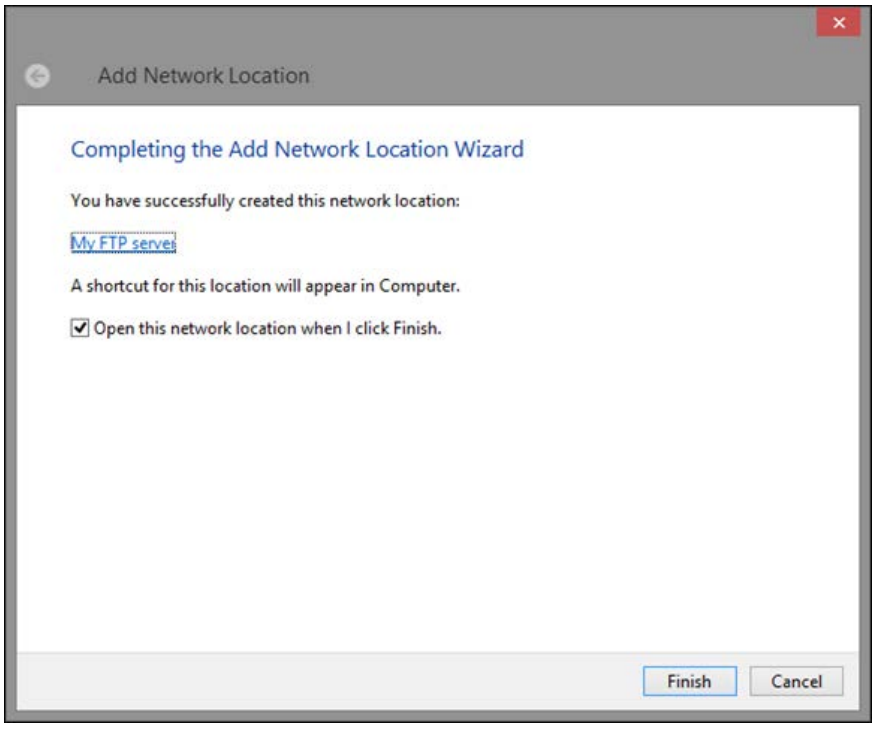
If you cleared “Log on anonymously”, you are asked to enter the user name for accessing the specified location. Type it and press “Next”.



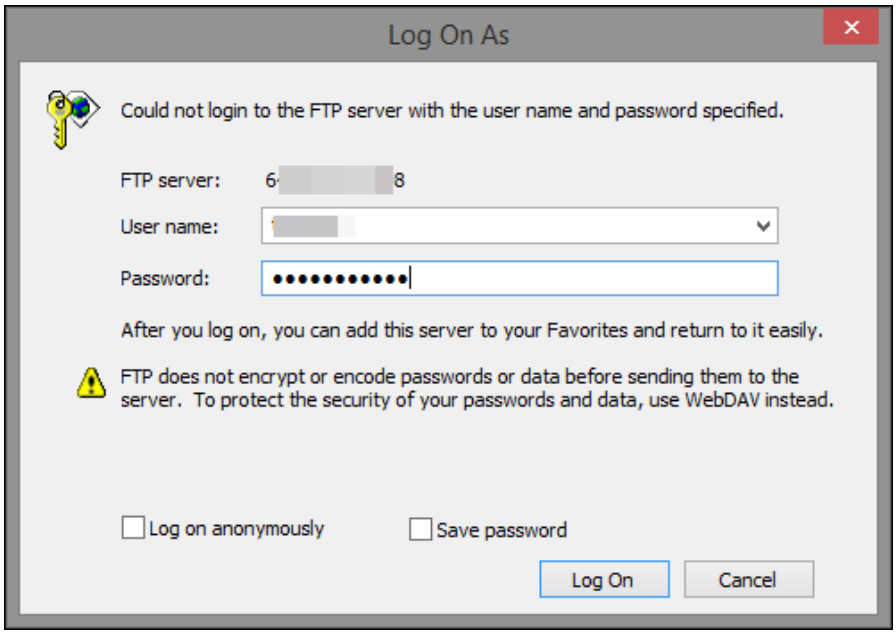
Now you are asked to give a *name* to this network location. Its default *name* is the IP address or the web address of the location you entered. Name it anything you wish and press “Next”.



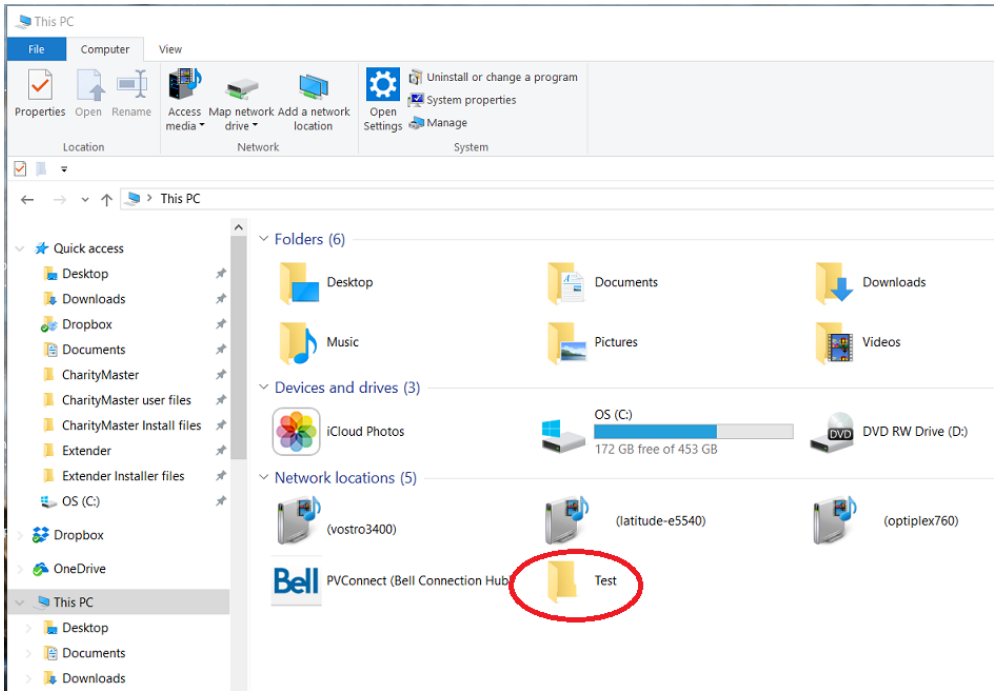
You are informed that you have successfully created this network location. Press “Finish” to access it.



If you can’t log on anonymously to this location, you will see the “Log On As” window, asking for the username and password to authenticate to this location. Type them and then select “Save password” if you don’t want to type the password every time you access this location. When done, press “Log On”.



The network location and its content is now displayed in an Explorer window.



You can now browse its contents and use it according to the permissions given to the user account you used to authenticate.