Forensic Filer Sync Setup 7/1/2010

There are 2 types of synchronization in Forensic Filer. Each one fits a specific network connection scenario.

If the laptops will always come back to the office and connect to the local LAN (via wired ethernet), then Forensic Filer will do a DIRECT sync. **With DIRECT sync, Forensic Filer Sync Server is NOT required**.

If the laptops will have the ability to connect to the LAN via a VPN connection, then Forensic Filer will do an INDIRECT sync. **With INDIRECT sync, Forensic Filer Sync Server is required.**

The full explanation and requirements of INDIRECT sync are given at the bottom of this document.

Setting up INDIRECT sync can only be done AFTER setting up Forensic Filer for normal network operation AND setting up DIRECT sync.

Forensic Filer must currently be installed on one or more desktop computers, with the database located on a mapped drive on a server? i.e. the database is located at F:\FFData\FFilerDat.mdb

Then at one of the desktop computers, you do the following to enable Sync: **You must have a license key for Forensic Filer Sync and have it registered .**

1. Open Forensic Filer
2. Click on "Utilities" menu
3. Click on "Forensic Sync"
4. Go to the "Sync Server Settings" tab
5. Click on the "Convert Database" button

Once this process is finished (it could take several minutes depending on your database size), you are ready to setup laptops.

The first phase in setting up a laptop is no different than the steps to setup a desktop workstation.

1. Start the Forensic Filer Installation program
2. Click Next
3. Select "Network Installation" and click Next
4. Select "Workstation Installation" and click Next
5. Click Next to accept the default installation location
6. Click Browse and navigate to your network database location   i.e. F:\FFData
7. Once the network path has been selected, click "OK" to close the Browse dialog
8. Click Next to accept the Network path
7. The License information should automatically be displayed
8. Click Next
9. Click Next to begin the file installation

Once installation is complete, start Forensic Filer on the laptop. It will automatically connect to the network database because you configured the network path in step 6.

These steps are the same for a new laptop or a new desktop.

To then set the laptop up for Remote operation (Sync), do the following on the laptop:

1. Open Forensic Filer
2. Click on "Utilities" menu
3. Click on "Forensic Sync"
4. Go to the "Sync Remote Settings" tab
5. Click on the "Create Remote" button

PLEASE NOTE - Once the remote file has been created (this may take a few minutes depending on your database size), you will need to exit Forensic Filer on the laptop and then go back in for Sync to be activated.

If your users are going to be using a VPN, you will need to setup the Sync Server and do additional configuration on the laptops. If this is the case, we will need to schedule a time to work together to get at least the first laptop setup for Indirect sync once you have the above steps finished, and have met the requirements for Indirect sync as listed below.

=== INDIRECT Sync ===

Requirements for using Forensic Filer Sync over a VPN connection.

1. The remote computer, once connected to the VPN, must be able to ping the "server" computer by name, not just IP address. This is because FF Sync uses a share on the server and the share is resolved by hostname.

2. Also, when the remote computer is connected to the VPN, the "server" computer must be able to ping the remote computer by name as well.

3. On the server, there must be a share that the remote computer has R/W rights to (this most likely already exists because the FF Data file is located on the server)

4. On the remote computer, there must be a share that the "server" computer has R/W rights to.

5. On the server, the FF Sync Server will run on startup. FF Sync Server is (at this time) unable to run as a Windows Service, so this means that the "server" must be logged in to the desktop as an administrator for FF Sync Server to run. Once it is running, the desktop can be locked for security purposes if you desire.

6. The FF Sync Server software must be installed on the server that hosts the Forensic Filer data files.

Here is how the new FF Sync works, which should explain the need for the above requirements.

The new Forensic Filer Sync uses a synchronization method called "Indirect Synchronization". What happens is that Forensic Filer on the remote computer (laptop) creates a Message File. It then transfers this Message File to a share on the server (i.e. \\Server\FFShare). The FF Sync Server monitors that share and upon seeing the Message File, opens it, processes it and creates a Response File. FF Sync Server then transfers that Response File to a share on the laptop (i.e. \\Laptop\FFShare). The laptop reads the Response File, processes it, and optionally creates another Message File and the process repeats. In a single Sync session, there are typically 2 or 3 back and forth exchanges of Messages and Responses depending on how many records in the database have changed since the last sync.

This is the reason that the laptop logged in user must have R/W rights to a share on the server, and the server logged in user to have R/W rights to a share on the laptop.

And, these rights and ping by name requirements are true whether the laptop is connected locally on the LAN in the office, or connected remotely over a VPN. The reason that I mention the VPN specifically is because many customers have previously setup VPN's where the laptops must map drives by IP address because they did not configure name resolution correctly, but on the local LAN, name resolution works fine. Hence, they have had to "fix" their VPN setup to get Forensic Filer sync working correctly over the VPN.

On a normal LAN using a real server (such as Windows Server 2003) with Active Directory, the rights are typically not an issue because most administrators will place the "Domain Admins" group into the "Administrators" group of every workstation, including laptops, so that any Domain Admin login has full rights to the workstation. In a non-standard "workstation is a server" scenario, additional, but similar, configuration is necessary to mimic the standard scenario.

Please describe the network and VPN configuration to help us understand your environment.

1. What OS is running on the Server
2. Is the server dedicated, or is it also a workstation
3. What device (Server or Router) is providing DNS on the network
4. Are you running WINS on the server?
5. What kind of Internet connection exists at the office (DSL, T1, etc)
6. What kind of Internet connection will the VPN users utilize? (DSL, Cellular Broadband, etc)
7. What VPN Hardware (Router) are you using
8. What VPN Client software are you using

Feel free to contact us with any questions you have regarding these requirements.