

FastTracker Fact Sheet: Laptops, Remote Users, and VPNS

If you will be activating laptops, remote users, or remote offices with the FastTracker service, this fact sheet will provide you with important information.

When deploying any Internet filtering solution to your employees, you first need to decide what network policies will apply to laptops, remote users, and remote offices.

How FastTracker Connects to your Network

FastTracker can connect to your network in several ways. One of the most common methods is by installing a 290Kb agent program called FPP on users' computers.

FPP is launched when a user logs into Windows. FPP configures all installed web browsers to use FPP as a proxy server. The user's web browsing passes through FPP, where it is tagged with ID information and forwarded on to the FastTracker Access Point (FAP). More information about setting up and using FPP is available at <http://www.fastdatatech.com/documentation/using-fpp.pdf>. When using FPP in an environment with laptops, remote users, and remote offices, there are some special considerations described below.

Note: If not using FPP, you should not be affected by VPN and roaming system (laptops) issues that occur with FPP. Without FPP, users are subject to network policy however the deploying customer sees fit.

Some Background about Dialup, RAS, and VPNS

There are many ways in which remote users and branches can access your corporate network. You likely use a combination of the mechanisms listed below:

- **Dialup** and **RAS** (Remote Access Service) involve a remote user dialing into a server inside your network with a modem. All web browsing originates on the user's machine, goes through the dialup connection into your network, then across your network and out to the Internet.
- **VPN** (Virtual Private Network) **tunneling** involve a remote user or branch accessing the Internet through a normal ISP connection, but using tunneling and encryption technology to access your internal network resources. Traditional VPNs behave just like RAS – causing web browsing to originate on the user's computer, go out to the ISP and into your network via the VPN tunnel, then across your network and out to the Internet.
- However, newer **VPN split-tunneling** causes only internal traffic to pass through the VPN tunnel to your network. In this case, web browsing originates on the user's computer, goes out to the ISP, and then directly to the Internet, without passing through your network.

With these different types of access technologies, you first need to decide under what circumstances you choose to monitor Internet usage.

Fast Data Technology's Recommendation

Fast Data Technology recommends that users be monitored and filtered when they are connected to your corporate network. On a case-by-case basis, this means that:

- **Laptops**
 - When the employee is in the office, filter.
 - When the employee is at home, but dialing into corporate RAS servers or using a VPN connection, filter.
 - When the employee is connected to a home ISP and not using a VPN connection, don't filter.

- **Home users**
 - If the employee uses RAS or VPNs to log into your network, filter.
 - If the employee is not logged into your network, don't filter.

- **Remote offices**
 - Always filter. Activate the offices as Branch Offices. More information about deploying to Branch Offices is available at: <http://www.fastdatatech.com/documentation/deploying-to-branch-offices-fact-sheet.pdf>

The table below describes how each of the connectivity cases should be handled.

You may choose to apply any variation of this policy.

Implementing Fast Data Technology's Recommendation

The key to implementing an on/off filtering policy is to only launch FPP in cases where the employee is to be filtered.

- **Login Scripts:** Using login scripts to deploy FPP makes turning on filtering when employees log into the network easiest. Since users only execute the login script when they connect to your network, they will only use FastTracker when they are connected to your network.

For laptops, login scripts should always be used in conjunction with the **Clear on Shutdown** feature in FPP. This feature causes FastTracker to turn itself off when the employee logs out. This ensures that when the employee takes the laptop home, it will not have FastTracker running until they log into the corporate network again.

Alternately, login scripts can be used in conjunction with the **Clear on Startup** feature in FPP. This feature causes FastTracker to turn itself off when the employee logs in to a machine when not connected into the corporate network.

To enable the Clear on Shutdown or the Clear on Startup features, make sure that the FastTracker configuration file, [fasttr.dll](#), contains the following lines:

```
[Security]
Clear on Shutdown=yes
Clear on Startup=yes
```

More information about the FastTracker configuration file is available at <http://www.fastdatatech.com/documentation/using-fpp.pdf>.

- **Workstation Installs:** If you are not using login scripts, FPP will launch every time the user restarts Windows. In this case, you must provide an icon that allows users to disable FastTracker when they are not using your network – however, they will be on their honor to use it responsibly. Otherwise, your only option is to have FastTracker always turned on, regardless of whether the employee is logged into your network or not.

If you have any questions that are not answered in this Fact Sheet, contact Fast Data Technology at support@fastdatatech.com.
