Are you installing i-Tree Eco within a computer network managed by an IT department with rules for software installation and website access? If so, please review and send the following to your IT managers so they can allow i-Tree Eco to run properly within your computing environment.

i-Tree Eco is a desktop software application that connects to and relies upon many HTTP, HTTPS, and FTP internet resources. It accesses the i-Tree website to display frequently updated content such as Adobe PDF files, as well as web mapping tools using Google Maps. It interacts with our server to enable multi-user field data collection via mobile web browsers on phones and tablets. It also submits and retrieves files for processing via FTP. **In order for i-Tree Eco to function, it should be treated as a web browser.**

The easiest method to ensure that Eco works is to enable User Prompting at the time of its installation. This will allow Microsoft Windows to prompt the user during its installation to allow Eco to access all the web resources it needs. On a regular Windows installation, Windows prompts the user whether or not to allow i-Tree Eco to access the Internet. When the user clicks “Yes” to this prompt, an exception will be automatically added to the user’s firewall that grants the i-Tree Eco executable access to the Internet regardless of port number or protocol.

This situation occurs because Microsoft does not maintain a consistent method of adding rules to the Windows Firewall from one version of Windows to the next. We apologize for this inconvenience, however there is little we can do to counteract it as we are be blocked by policy settings in managed networks.

The more difficult method is to add an exception to the user’s firewall that grants complete access to the Internet for i-Tree Eco executable. Targeting explicit domain names, port numbers, or IP addresses is not recommended because we cannot guarantee that we will not add or modify them in the future. *The best way for an IT department to discover the appropriate rule is to install the software on a machine with the prompt enabled and then copy/duplicate the rule generated by Windows into their corporate firewall policy.* i-Tree Eco has two (2) executables (32 and 64 bit) so a rule should be generated for each to ensure it runs correctly on all installed computers.

As noted, i-Tree Eco uses FTP, HTTP, and HTTPS to communicate with our servers. FTP by nature of the protocol requires UDP as well as TCP in order to function properly. HTTP and HTTPS both currently use TCP only. An IT department can thus choose to create a rule for each i-Tree Eco executable that permits the Eco application to use ANY protocol, or they can choose to create additional rules to allow only UDP and TCP traffic for each executable. If you decide to try and set up Firewall rules, the following maybe effective for you at the time of this writing:

Address/Host	Application Protocol	IP Protocol	Ports
*	HTTP	TCP	80

*	HTTPS	TCP	443
*	FTP	TCP	20, 21

FTP uses two TCP connections. The client, i-Tree Eco in this case, initially connects on port 21 to our server to establish a command connection. In an active FTP session, the server would attempt to connect back to the client on TCP port 21. Due to Network Address Translation, aka NAT, this is typically not possible because the public IP address from the view of the FTP server is not the IP address of the client. Because of this, i-Tree Eco resorts to passive connections where the server opens an additional TCP port and tells the client via the currently established command connection on port 21 which port to connect to. Without special software to intercept FTP traffic and to dynamically add rules to allow the client to connect to the server on the specified port, the client must be permitted to connect via TCP to ALL ports on the server. It should be noted that these are the same rules that modern web browsers require to function. However, browsers such as Chrome have already begun to use other application protocols which add additional IP protocols and ports to the mix.

The above may too permissive for some organizations. For those organizations, they can limit the rules to the i-Tree Eco application only, just like they do for an installed web browser. The recommended rules for the **Windows Firewall** are:

Type	Executable	Profile	Remote IP	IP Protocol	Port
Outbound	i-Tree Eco v6.x86.exe	All	Any	Any	Any
Outbound	i-Tree Eco v6.x64.exe	All	Any	Any	Any