Network Requirements for the USPTO/Direct Client

The USPTO/Direct client requires the ability to directly communicate with special USPTO Internet servers using TCP/IP port 443 at each login and during the creation, recovery, or update of a profile. These servers are part of the USPTO's Public Key Infrastructure (PKI) that manages the digital certificates issued by the USPTO. It is important to note that for these operations, the USPTO/Direct client **does not use** the proxy settings of your browser. If direct access to servers (through a firewall or proxy) using port 443 is prohibited in your environment, see Alternate ports supported by USPTO/Direct below.

Once the Direct client has successfully logged in, it automatically launches the default browser for the workstation and uses its proxy settings when accessing the USPTO or other web sites.

Alternate ports supported by USPTO/Direct

By default, the USPTO/Direct client is configured to use TCP/IP port 443 for communications with the USPTO's PKI servers. TCP/IP port 443 was chosen as the default because in network environments where firewalls are in use, client workstations are normally allowed to access servers on the Internet using this port. However, in environments where proxy servers are used, or a combination of firewall and proxy server, it is often undesirable to enable direct communication on port 443 through the firewall. For this reason, the USPTO Direct client may be configured to use an alternate set of ports for communicating with the USPTO's PKI servers. These alternate ports are port 389 for communicating with the USPTO's Directory servers, and port 709 for the Certificate Authority. To configure Direct to use these ports, make the following changes to the entrust.ini file located in the C:\Program Files\USPTO directory:

Change:	To:
[Entrust Settings] ClientType=Heavy Server=dir-01.uspto.gov+443 Manager=ca-01.uspto.gov+443	[Entrust Settings] ClientType=Heavy Server=dir-01.uspto.gov+389 Manager=ca-01.uspto.gov+709

After saving the changes to the entrust.ini file, restart the USPTO Direct client to use the new configuration.

Common problems with the USPTO/Direct Client in environments where Proxy Servers are used

In network environments where proxy servers are used, the proxy server and/or firewalls are often configured to prevent direct access to servers on the Internet

or to restrict access to specific types of network traffic by TCP/IP port number. In some environments, proxy software is loaded on each client workstations so applications requiring direct access will work transparently with the proxy server.

In environments where proxy client software is not used, customers will need to contact their network administrator or information technology support staff for assistance in configuring their environment for the USPTO/Direct software.

Customers may want to restrict access in their firewalls to our IP address only for specified ports. The IP addresses are as follows:

Server= 63.71.228.204 on port 389 Manager=63.71.229.67 on port 709

Why does the USPTO/Direct Client need to access the dir-01.uspto.gov server every time I login in?

The Direct client retrieves a Certificate Revocation List (.crl file) and Policy Certificate (.pch) during the login process to verify the customer's digital certificate is still valid. These files are valid for a period of time (usually no more than a couple of days) so a login will succeed if communications with the USPTO Directory Server is not possible but the files are present and have not expired. The user may experience a noticeable delay during the login while the client attempts to communicate with the USPTO Directory server before the login completes. If a login is attempted after the files have expired, a message indicating the **Attribute Certificate is missing or invalid** or **Unable to Initialize USPTO Direct - Failed to Initialize Public Directory** will be displayed and the login will fail.