

stickapp vpn client

powered by *portablevpn*

Installation & Configuration Guide

This document is provided to guide you through the process of installing and configuring StickApp VPN Client when used on SafeStick's managed by SafeConsole.



Overview

StickApp VPN Client is one of a number of Security and Productivity apps available for SafeStick, managed by SafeConsole's Publisher Feature. The VPN Client enables secure, authenticated remote PPTP VPN access to private networks such as your office network or branches anywhere in the world.

Having your VPN client installed on a SafeStick makes VPN more secure, as if an unencrypted laptop for example is stolen, then the thief would be able to use the installed VPN client and connect to your office.

Administrators can pre-configure, deploy and change all settings centrally at any time making user error virtually impossible.

CRITICAL NOTE: You **MUST** have followed the "StickApps Technical Installation Guide" which walks you through configuring SafeConsole and enabling the Publisher and Autostart features. **You absolutely must do this** before any StickApp will run on SafeSticks. If you have not done so please do this before proceeding with this document.

StickApp VPN Client System Requirements

- Microsoft Windows XP, Windows Vista or Windows 7
- Approximately 4Mb available space on a users SafeStick.
- A PPTP VPN capable firewall / host / device which is configured to accept such connections. (Not covered in this document).
- StickApp VPN Client has been tested with many firewalls including Sonicwall, Astaro, Draytek, Vigor, Cisco, Buffalo and many more. It should work with any which support PPTP. Contact your firewall vendor for advice.

Licence

A trial licence for StickApp VPN Client is provided automatically which allows connections time limited to 5 minutes. For continued licenced use you must purchase a subscription. All licenced applications are fully supported.

Installation

From the StickApps VPN Client download package, extract the "VPNClient" folder to a temporary local folder on your desktop or hard drive – for example c:\TEMP\vpnclient. It **MUST** be a local drive for configuration.

Run the "NetworkClient.exe" application from the vpnclient subfolder – for example;

c:\TEMP\vpnclient\vpnclient\NetworkClient.exe

You can then configure the required settings as discussed on the following pages before Publishing to your SafeSticks.

Any time you wish to change these settings, you should perform this step before copy the updated settings files to the Published location.

The Application

This is the main window for the client, if it is the first time it is being run then the settings and the end user licence agreement windows will be displayed.



Settings Window

The settings can simply be accessed or changed by clicking on the settings button on the main application window.

The settings are made up of several tabs each of which is self explanatory.

VPN Details / Settings / DNS Tabs

These tabs are where you will configure the username, password and VPN server address for the VPN connection as well as various compression, encryption and other settings.

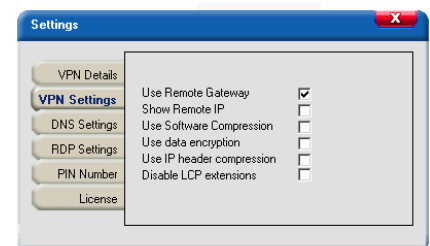
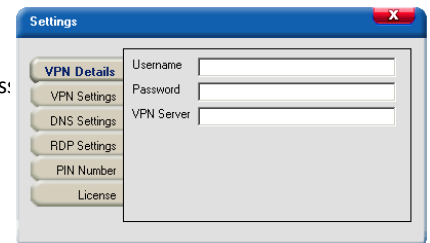
The VPN Server address can be either an IP address or a valid DNS name of the VPN Server.

You can also enable the other options as appropriate for your environment and requirements.

To use the remote network for all network traffic the use remote gateway option should be checked. If you wish to know on the main client window what address you have been assigned by the server then check the show remote IP option.

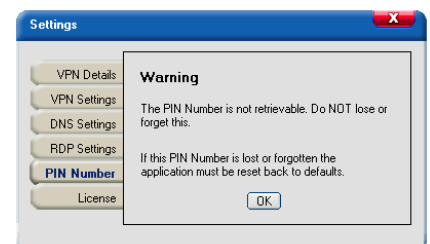
NOTE: It is we believe acceptable to use the same username and password details for all of your VPN users for several reasons;

- 1) It is easy to disable individual users SafeSticks – you can either disable the user account in Active Directory, or disable the SafeStick directly in SafeConsole. SafeConsole will then lock down the SafeStick preventing further VPN connections.
- 2) You can un-publish the entire VPN Client at any time
- 3) You can change the username / password and push the new settings down to only valid SafeStick users at any time.



PIN Number Tab

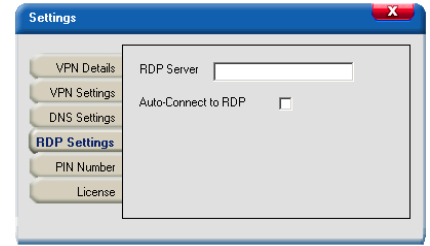
Using the PIN Number tab you can also select to require a PIN number which must be entered before the connection is established, and for modifying the settings – however this probably will not be required as the application is running from a secure SafeStick.



Remote Desktop (RDP Settings) Tab

The RDP Settings tab will allow you to enter a server on the remote network that uses remote desktop (RDP) that you may want to connect to.

Again, this can be an IP address or FDQN – fully qualified domain name.



Licence Tab

On this tab you can enter your permanent licence key as supplied which will give you the fully licenced version of the VPN client.

Connect

To test the connectivity, simply click connect.



Publishing the VPN Client via SafeConsole

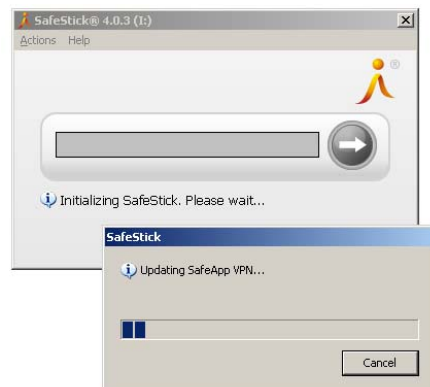
Once you have configured the VPN Client and tested it locally, you can then Publish it for use on your SafeSticks.

- Copy / move the locally configured VPN Client folder and subfolders from you local drive - for example C:\TEMP\VPNClient\ to your Publisher UNC share path – for example \\myserver\publisher\vpnclient

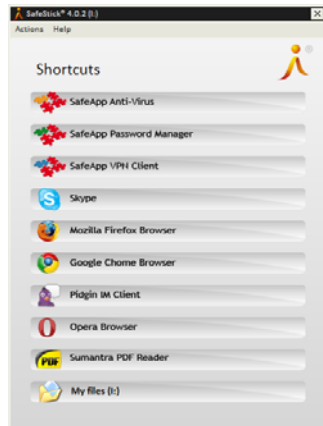
NOTE: In the Publisher UNC share you must now have \vpnclient which contains “vpnlauncher.exe” AND you will also have a sub folder also called vpnclient “\vpnclient\vpnclient” – which contains the program, settings and other necessary associated files.

- Done !

The next time a SafeStick is unlocked by a user in the OU Group you have specified for Publisher, the VPN Client will be downloaded onto their SafeStick automatically, into a sub-folder of the <safestick drive letter>\Applications folder.



“StickApp VPN” will also appear automatically in the users SafeStick ShortCut menu.



Un-Installing StickApp VPN Client

StickApps are easily uninstalled – either individually or all installed StickApps completely - from users SafeSticks.

Option 1.

To remove ALL StickApps, start SafeConsole and disable the Publisher policy completely, or edit the Publisher policy from a selected OU Group as required.

The next time SafeSticks poll into SafeConsole to obtain policy, they will “know” that Publisher has been disabled and will delete all files from the <safestick driver letter>\Applications folder completely. Shortcuts will also be removed.

Option 2.

From your published share – for example [\\myserver\publisher](#) delete one or more StickApp folders as required. So to remove VPN Client simply delete entirely the [\\myserver\publisher\vpnclient](#) folder.