# FortiClient SSL VPN Client User's Guide

To connect to Model Driven Solutions via a SSL VPN Client session you first need a VPN login account that has been granted the proper SSL VPN group permissions and associated password. To obtain a VPN account or to reset your password, please contact your systems administrator.

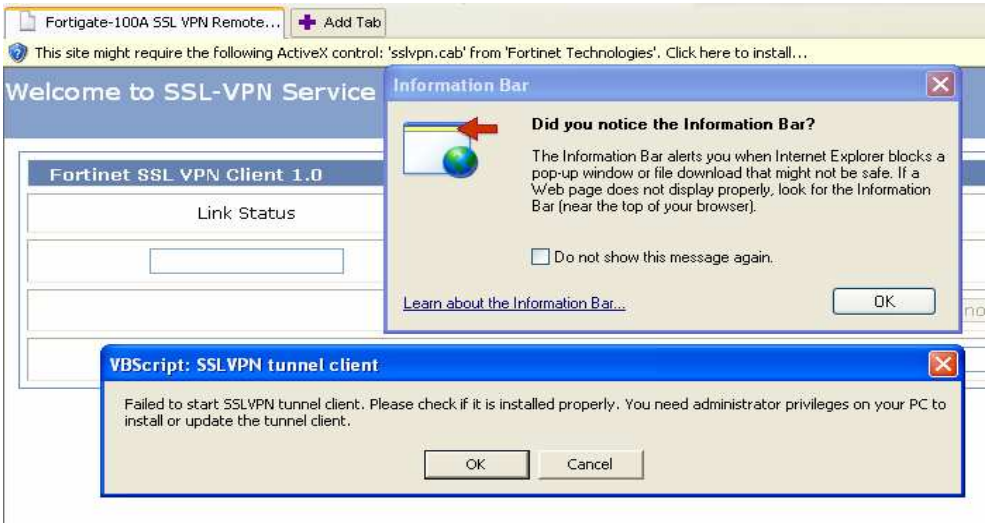
You can establish a SSL VPN tunnel connection to MDS by either using the web browser plug-in or by installing the stand alone client application both of which currently support: "Microsoft Windows 2000/XP/2003 or Vista (32 or 64-bit), MacOS X v10.3.9, v10.4 "Tiger", v10.5 "Leopard", or Linux Distributions RedHat/Fedora,Ubuntu/Debian, or Suse." Currently supported browsers include: "Microsoft Internet Explorer 6.0 (or later), Netscape Navigator 7.0 (or later), Mozilla Foundation/Firefox 1.5 (or later), or Apple Safari 1.3 (or later)." As of the time of this writing I have only had success using the browser plug-in though Windows using IE 6 or IE 7 and had no Mac platform available for testing. Hopefully, future Fortinet firmware updates will resolve these issues. To install either the browser plug-in or stand alone SSL VPN Client you must have administrator/root privileges on the client computer.

### Installation of the FortiClient SSL VPN browser plug-in client

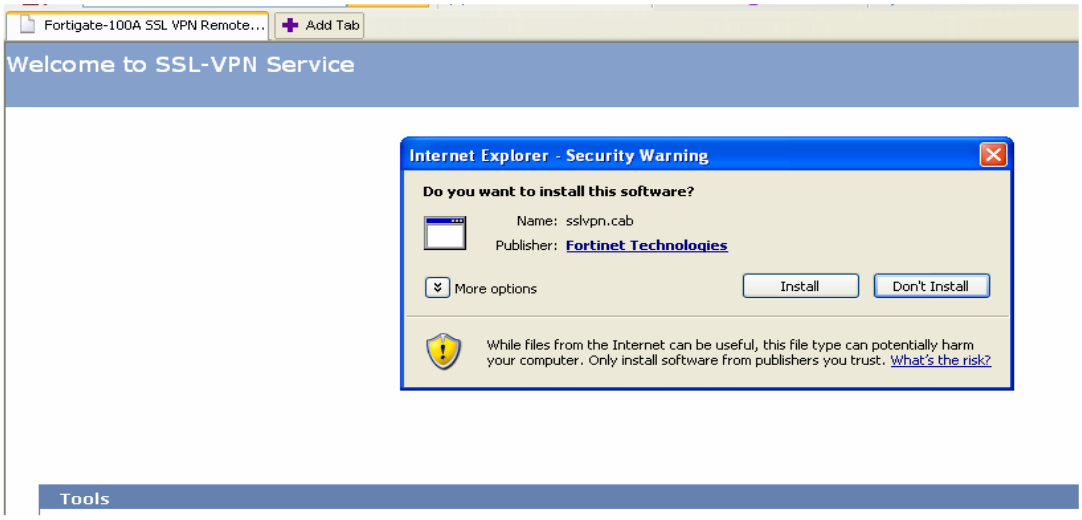
1. Open a web browser session and connect to the following URL: https://vpn.enterprisecomponent.com:10443 , please note that the current SSL cert is self signed, accept it to continue.
2. You will be presented with the following form, login to proceed.


3. After login you will see the initial web portal page, click on the 'Activate SSL-VPN Tunnel Mode' link to begin installing the software.

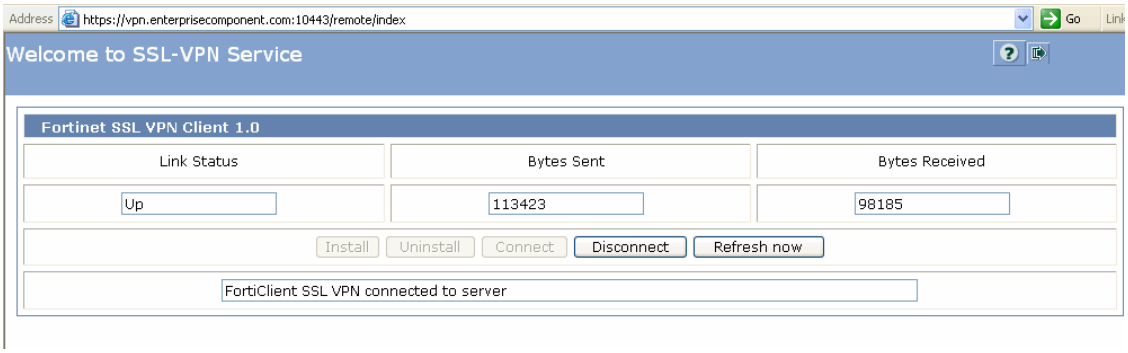
4. The software includes both an activeX control and the Fortinet client, accept installation of the activeX control first.




5. After the installation of the activeX control completes click on the 'Activate SSL-VPN Tunnel Mode' link again to install the fortinet client configuration.




6. After the installation of the fortinet client completes the SSL VPN tunnel should connect automatically. If not you may need to re-establish your login to the web portal and click on the 'Activate SSL-VPN Tunnel Mode' link again. Please use the button located at the top right of the web portal form to log out of a SSL session.



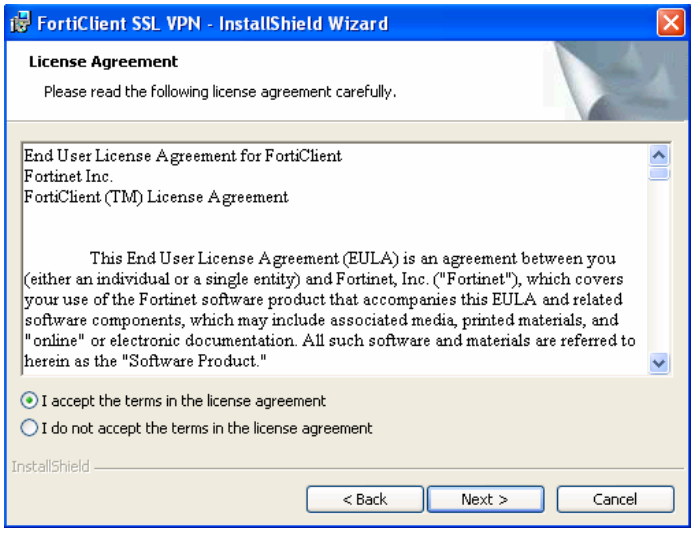

7. Now that the required software is installed you can access the MDS internal network by connecting to the SSL VPN web portal using your browser and clicking on the 'Activate SSL-VPN Tunnel Mode' link, https://vpn.enterprisecomponent.com:10443 .

**Installing the stand alone FortiClient SSL VPN Client for Microsoft Windows**

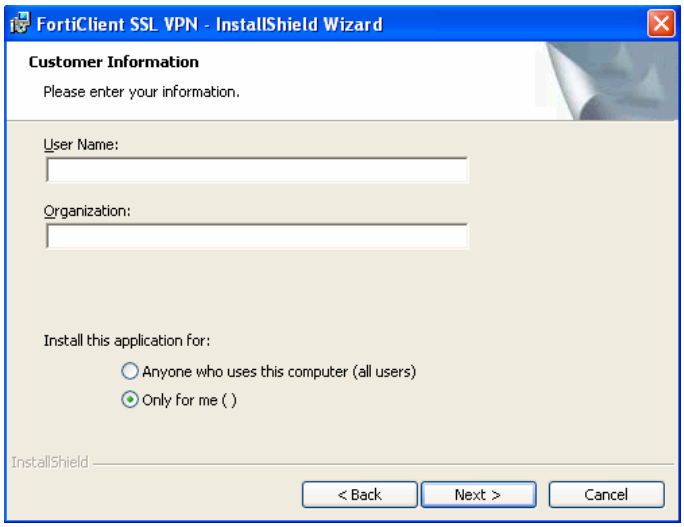
1. Click on the following links to run or download the FortiClient SSL VPN installable appropriate for your Windows 32/64 bit operating system: '*.msi' or '*.exe'. Use the '*.exe' version if your OS doesn't have support for the "Microsoft/Windows Installer", either will work on most systems.
   EXE:
   http://internal.enterprisecomponent.com/download/FortiClientSSLVPN/SslvpnClient_4.0.2010.exe
   MSI:
   http://internal.enterprisecomponent.com/download/FortiClientSSLVPN/SslvpnClient_4.0.2010.msi

2. After starting the installation process you will first see the welcome screen, click on 'Next >' to continue.

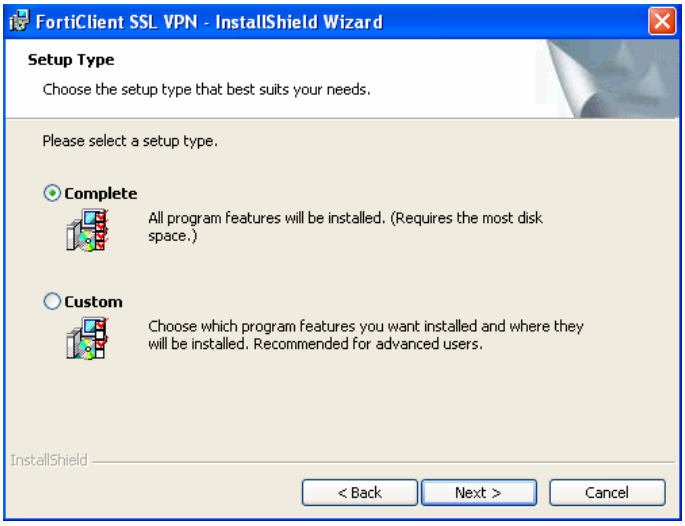

3. Next you will be presented with the FortiClient license agreement, you must accept the license terms to install the client, click on 'Next >' to proceed.



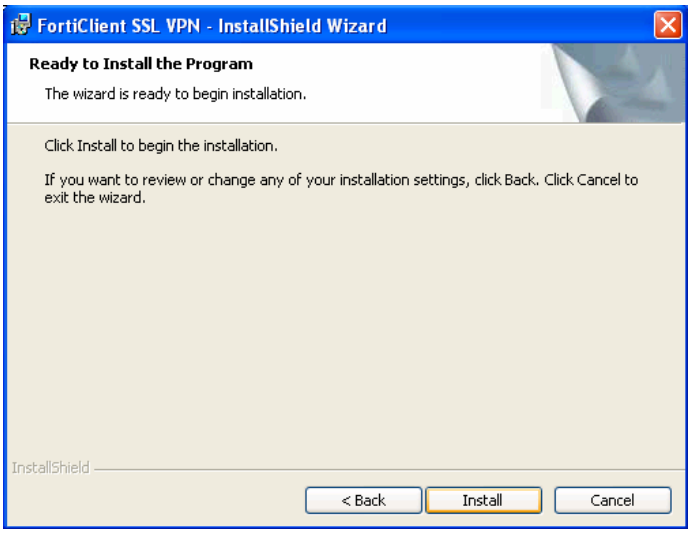

4. The following form requests a user and organization name for the license registration. Please select the ‘Only for me ( )’ option button on shared computers, click ‘Next >’ to continue.



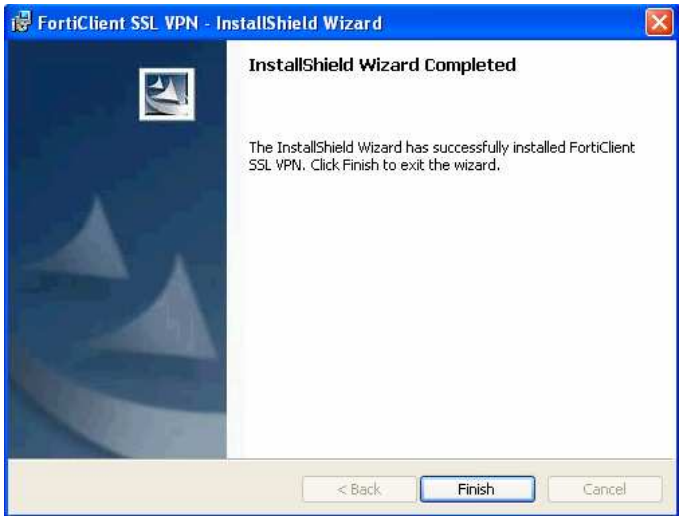

5. On the installation ‘Setup Type’ form select ‘Complete’ and click on ‘Next >’.



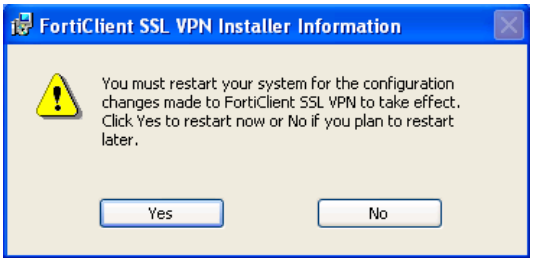

6. Click on the ‘Install’ button to begin the installation.



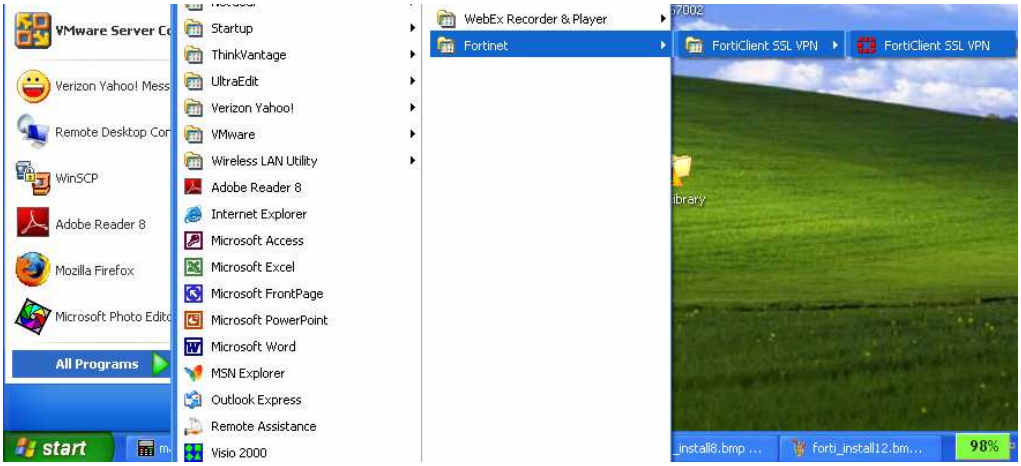

7. When the installation setup completes click on the ‘Finish’ button.




8. Finally, it is requested that the system be restarted to complete the installation.

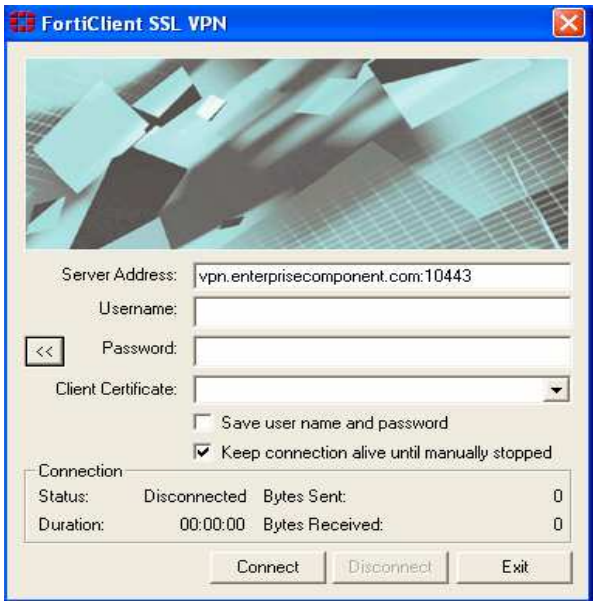



9. By default a program link is created in ‘Start->All Programs->Fortinet->FortiClient SSL VPN’.




10. Launching the client application opens the following window. Enter the ‘Server Address:’ as shown, vpn.enterprisecomponent.com:10443 , followed by your login name and password.


11. Click on the >> button to display more user options such as the caching of login credentials and persistent connections. We are not currently using client certificates so leave that field blank.




12. After establishing a SSL VPN tunnel the program screen will display the connection statistics and runtime icons in the system tray.

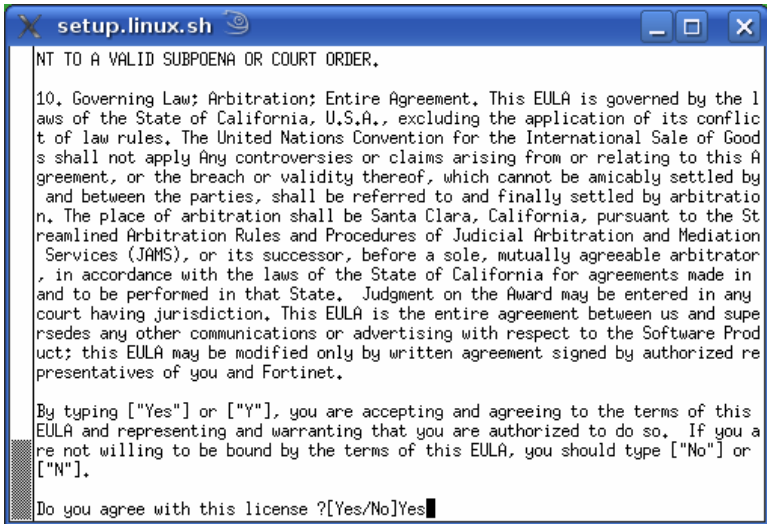

**Installing the stand alone FortiClient SSL VPN Client for Linux**

1. Download the Linux archive file by clicking on the link below. Please note that this client requires the X11 GUI environment and pppd, point to point protocol daemon, to work.
   http://internal.enterprisecomponent.com/download/FortiClientSSLVPN/forticlientsslvpn_linux_4.0.2010.tar.gz

2. Decompress the archive using the X-11 GUI or by issuing the following command:
   tar –xzf forticlientsslvpn_linux_4.0.2010.tar.gz

3. Move into the decompressed folder using the X-11 GUI or from the command line: cd forticlientsslvpn

4. Launch the client by executing the forticlientsslvpn binary. The first time the client is run it launches the setup.linux.sh configuration script which, prompts for acceptance of the license agreement. Tap the space bar to scroll though the EULA. Type in ‘Yes’ and press the Enter key to accept the license terms and launch the SSL VPN client.




5. For the ‘Server:’ field enter vpn.enterprisecomponent.com : 10443 as shown along with your user login and password.


6. Clicking the 

button displays more client settings such as saving login credentials and persistent connections. We are not currently using client certificates or a proxy so leave those options unchecked. Click on the  button to close the ‘Advanced Settings …’ window and return to the client.


7. Clicking on the Connect button establishes a SSL VPN tunnel and changes the status bar from 'Ready' to 'Tunnel running' as well as displaying the connection statistics.