IT Department: Instructions on VPN Connection to the SoftServe University Network Using AnyConnect VPN Client

User Guide

Version 1.0

04.12.2013

SoftServe

Revision History

Date	Version	Description	Author
04/12/2013	1.0	Document creation	Ihor Kohut

1 VPN Access Overview

VPN technology (Virtual Private Network) enables mobile and remote users to set up secure connections to the company main office network. The advantage of VPN access is that a user with the VPN connection to the company network can work in the same network environment as if the computer is directly connected to the local network on the work place. To create such connections, user just needs Internet access: dial-up, DSL, or cable; and there is no need to perform long-distance calls or rent data transfer channels.

This guide describes the usage of SSL VPN (Secure Socket Layer VPN). This technology provides the possibility to ensure a high-level security using traffic encryption and authentication. In order to establish VPN connections to corporate network, Cisco AnyConnect VPN Client (VPN Client) must be installed on the client's computer.

1.1 Instructions on Using VPN Access to the SoftServe University Network

1.1.1 Access policies

SOFTSERVE UNIVERSITY login username and password are used for authentication of the remote access.

The VPN access security is configured in the way that users, when setting up the VPN connection, are assigned to predefined remote access groups

By default, when user is connected to the VPN gateway, only the traffic from and to the SoftServe University resources is routed via VPN tunnel. The rest traffic is sent via general Internet connection and it is not secure.

2 VPN Client Installation

2.1 Prerequisites and supported platforms

Corporate VPN client (Cisco AnyConnect 2.5) is supported on the following OSs:

OSs	Notes:
Microsoft Windows AnyConnect 2.5 supports the following Windows OSs: • Windows 7 on x86 (32-bit) and x64 (64-bit) AnyConnect requires a clean install if you upgrade from Windows XP to Windows 7. • Windows Vista on x86 (32-bit) and x64 (64-bit)—SP2 or Vista SP1 with KB952876. AnyConnect requires a clean install if you upgrade from Windows XP to Windows Vista. • Windows XP SP2 and SP3.	Requirements • Pentium class processor or greater. • x64 (64-bit) or x86 (32-bit) processors. • 5 MB hard disk space. • RAM: – 256 MB for Windows XP. – 512 MB for Windows Vista. – 512 MB for Windows 7. • Microsoft Installer, version 3.1. If you are using Internet Explorer, use version 5.0, SP2 or later. For WebLaunch, use 32-bit Internet Explorer 6.0 or later, or Firefox 2.0 or later, and enable ActiveX or enable Sun JRE 5 Update 1.5 or later (JRE 6 recommended) AnyConnect is compatible with 3G data cards which interface with Windows 7 via a WWAN adapter.
Apple AnyConnect 2.4 supports the following versions of Mac OS: • Mac OS X 10.5 • Mac OS X 10.6.x (32-bit and 64-bit).	50 MB hard disk space required.
Linux AnyConnect supports the following distributions: • Red Hat Enterprise Linux 5 Desktop • Ubuntu 9.x	AnyConnect supports only standalone installations on Linux. See the AnyConnect Linux Requirements for AnyConnect 2.5.

To install AnyConnect through a web browser (WebLaunch), the user platform must match one of those in the table:

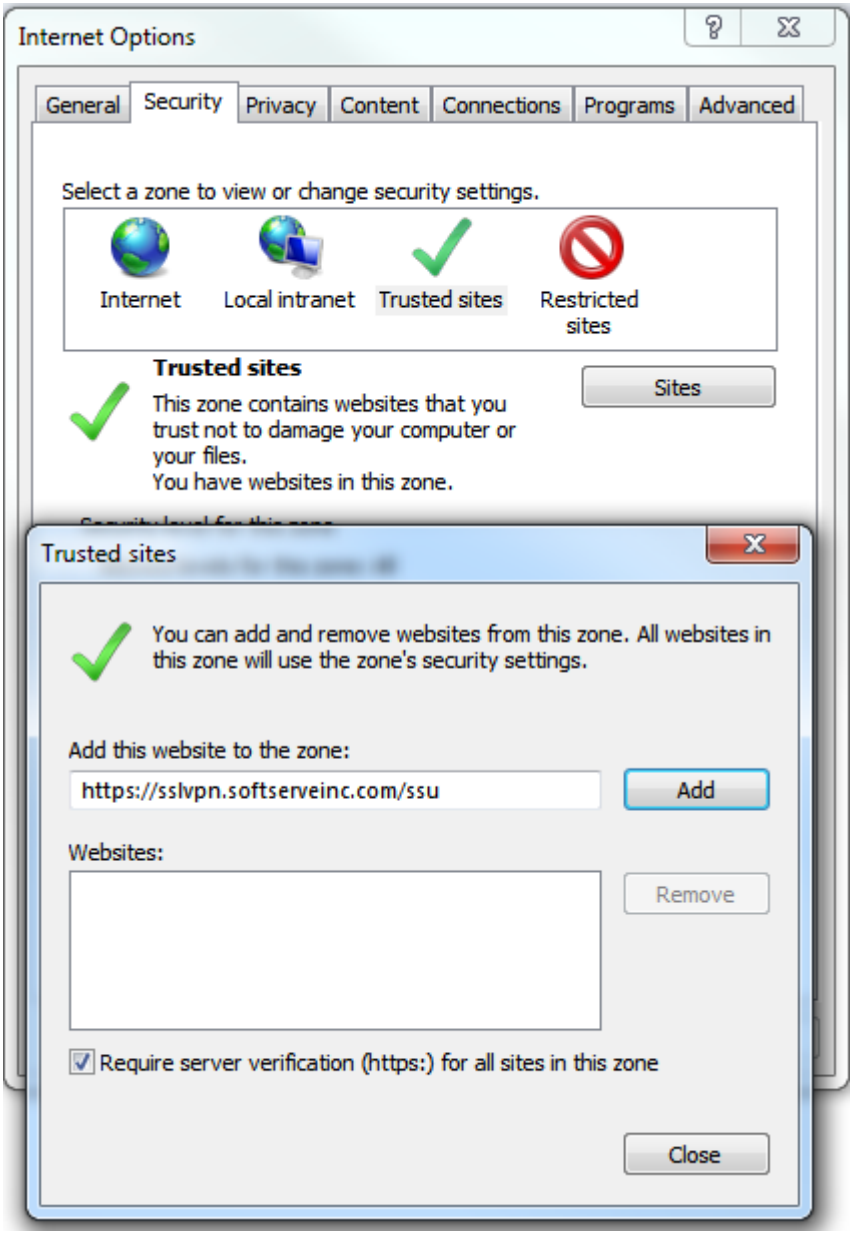
OSs	**Browsers**
Windows 7 on x86 (32-bit) and x64(64-bit)	Internet Explorer 8.x Firefox 3.x
Windows Vista on x64	Internet Explorer 7.x/8.x, Firefox 3.x
Windows Vista SP2 on x86 Vista SP1 with KB952876 or later on x86	Microsoft Internet Explorer 7 Firefox 2.0 or later
Windows XP on x64	Internet Explorer 7.x and 8.x Firefox 3.x
Windows XP SP2 or later on x86	Microsoft Internet Explorer 6.x-8.x Firefox 2.0 or later
Apple: Mac OS X 10.5	Safari 2.x Firefox 3.x
Mac OS X 10.6.x 32- and 64-bit	Safari 4.x Firefox 3.x
Linux	Firefox 2.0 or later

Use only the 32-bit version of Internet Explorer or Firefox to install VPN client. (At this time, Firefox is available only in a 32-bit version.)

The AnyConnect VPN Client requires either **ActiveX** or **Java** to use the web-based connection/install. For ActiveX, the user will need to have permission to install into their web browser (or it can be pre-installed). If ActiveX is not supported or used, Java is attempted. The version can be 1.4.x or 1.5. The Java implementation is an applet and is browser-based (no download).

On the first connection, the ActiveX/Java would be used to install the AnyConnect VPN Client software. This requires **admin rights**. Subsequent connections do not require admin rights (even for client upgrades). The client has a standalone installer for cases where admin privileges are not granted to the user.

When using Internet Explorer, VPN alliance's address (https://sslvpn.softserveinc.com/ssu) must be added to the list of trusted sites in order to ensure correct insta llation process and to avoid extensive interact ion from user. Following screenshot shows h ow do add address to "Trusted Sites" (Tools > Internet Options > Secu rity > Trusted Sites > type in " https://sslvpn.softserveinc.com/ssu" > Add).



AnyConnect does not support virtualization software such as VMware and Parallels Desktop.

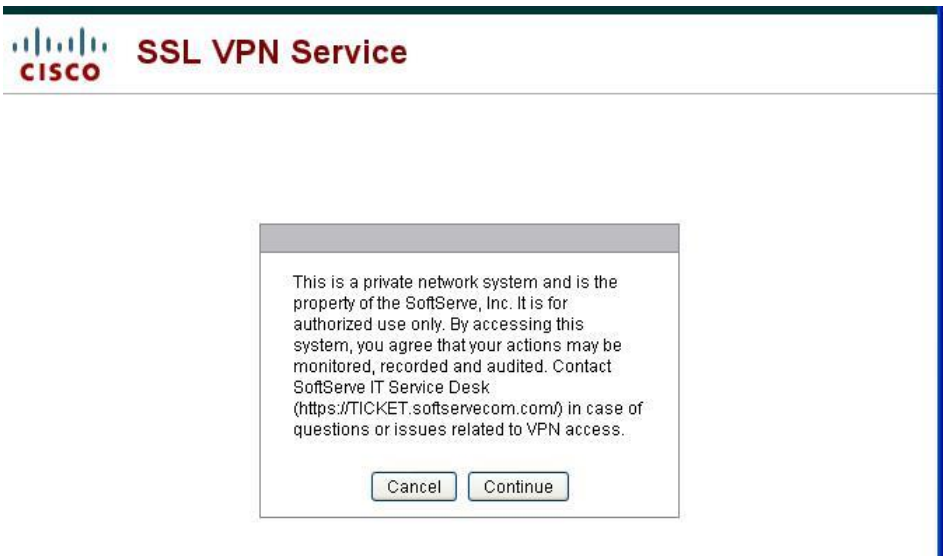
2.2 Web-based installation

Main method for VPN client deployment is Web-based installation. Without a previously-installed client, remote users enter the corporate VPN gateway address – https://sslvpn.softserveinc.com/ssu – in supported browser.
After entering the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, he downloads the client that

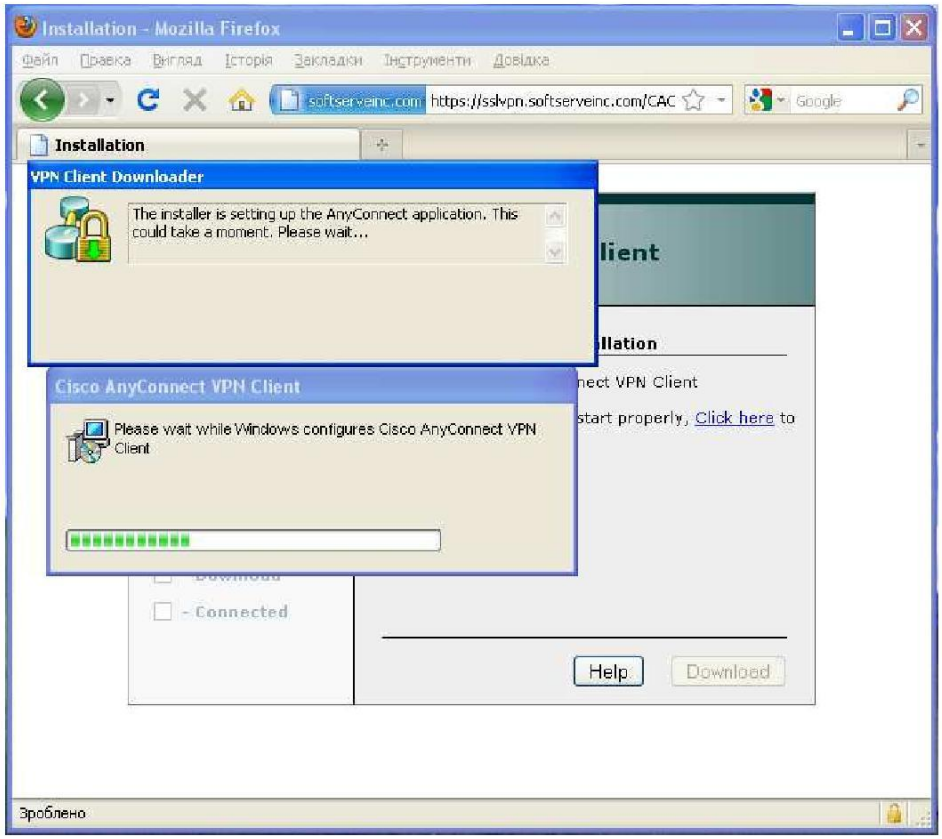
matches the operating system of the remote computer. After downloading, the client installs and configures itself and establishes a secure SSL connection.
Following screenshots illustrate web-installation process.

- Open https://sslvpn.softserveinc.com/ssu in browser and enter login credentials in authentication form

- Accept security warning



- VPN gateway detects OS, corresponding VPN client is being downloaded and installation launched

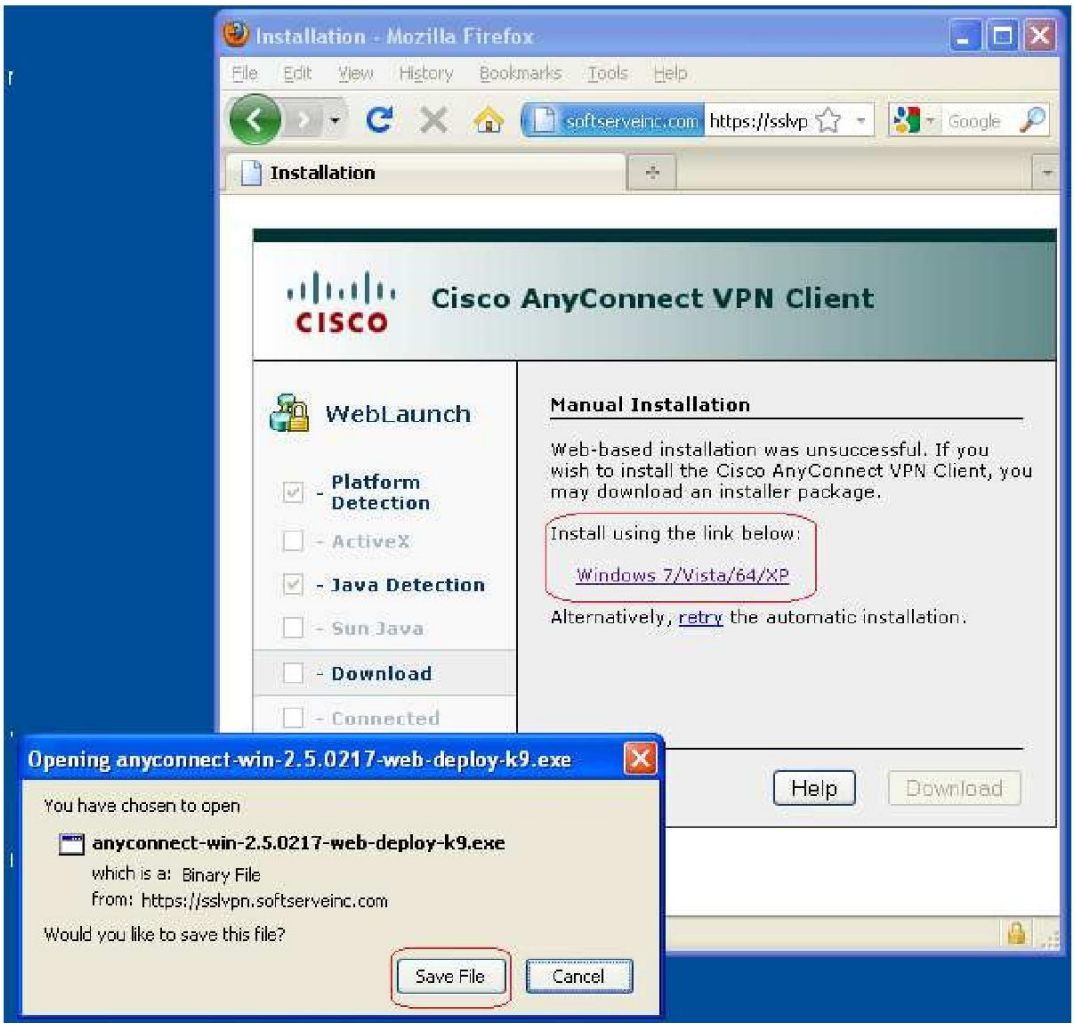


- AnyConnect VPN client icon is indicated in system tray upon successful installation and connection.

Subsequent connections can be made either by launching “Cisco AnyConnect client” application from “Start” menu or by opening VPN gateway’s address (https://sslvpn.softserveinc.com/ssu) in browser.

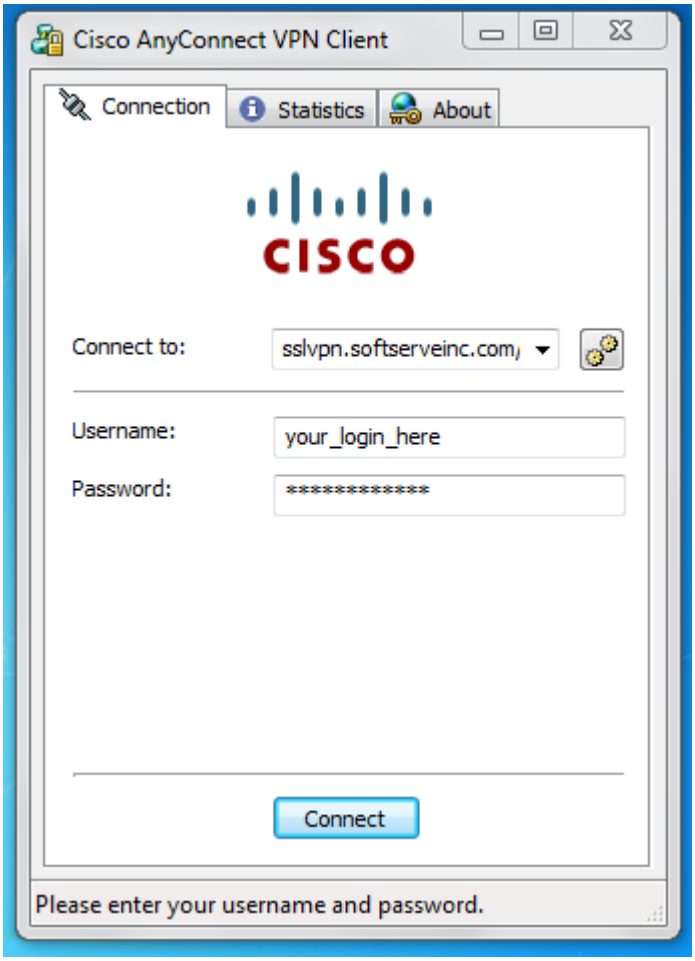
2.3 Manual installation

Under some exceptional conditions like disabled ActiveX or Java applet execution automatic WebLaunch process may fail and user is proposed to manually download and install AnyConnect VPN client as shown on the screenshot below.



User should download and run executable file and follow installation dialog.

After successful automatic or manual installation AnyConnect client application can be launched from “Start” menu for subsequent connections. Next screenshot shows application window.



VPN client does not require any configuration from user; all parameters are applied centrally from VPN gateway upon connection based on user attributes in central authentication database.
There are only three fields for input from user. “Connect to:” field indicates VPN gateway address, it is nor mally predefined after automatic installation but if address was deleted or empty for any reason user should enter “ **sslvpn.softserveinc.com/ssu**” in this field. “Username:” and “Password:” prompt appears during c onnection establishment phase. SoftServe domain userna me and password should be submitted respectively.

In cases when there is no access to VPN gateway’s web-interface, VPN client can be downloaded from corporate Portal.

3 Troubleshooting

If you are experiencing problems with your VPN client installation or connection to the SoftServe corporate network, you should check the following:

- VPN gateway address should be referenced only by URL https://sslvpn.softserve**inc**.com/ssu, do not confuse with sslvpn.softserve**com**.com/ssu as it will lead to errors during connection.
- Your Internet connection should function properly prior to establishing the VPN connection. If you have problems with your Internet connection (losses), it may cause VPN disconnection issues.
- When connecting from networks protected by firewall, make sure that TCP and UPD traffic by destination port #443 to VPN gateway is permitted. If only TCP connections to port 443 are permitted this may reduce VPN connection performance. UDP must be permitted as well.
- AnyConnect client is not compatible with Windows Network Connection Sharing. It may be indicated by error message "The VPN client agent was unable to create the inter process communication depot". Check Control Panel Network connections Local Area Connection Properties Sharing and clear all options.
- The AnyConnect SSL VPN Client can use a configured proxy server in your browser (IE only). However, when it connects, it does not negotiate a Datagram Transport Layer Security (DTLS) User Datagram Protocol (UDP) tunnel. Only TLS TCP is used when you connect this way thus connection performance may be reduced and applications which require real-time traffic exchange (like IP phone) may not function properly.
- Avoid using addresses from range of 192.168.X.X in your home network as they can overlap with corporate addresses and this can lead to inability to connect to certain resources.
- Some personal firewall and antivirus software may block VPN client application and its traffic. You should add AnyConnect client to the list of trusted applications for such antiviruses.

If you need help with corporate VPN access please submit ticket to IT department.