Installing the Cisco AnyConnect Secure Mobility Client

Overview:

Sunrise™ Exchange uses a Virtual Private Network (VPN). Connecting to a remote corporate server, using the Internet, the VPN allows connection between Insurers and Intermediaries to operate in a secure manner. The Sunrise™ Exchange VPN is based on the IPSec protocol and takes advantage of the broad availability of the Internet. IPSec encrypts everything between two computers. Using a VPN connection, data is carried over the public network, but is unreadable to unauthorised clients. It also provides audit records to show access information.

You will be provided with new Usernames and Passwords to download and access this software for each machine requiring connection to Sunrise Exchange. This information is listed on your **Sunrise Configuration Sheet**.

If you have not received your login information, please contact support@ebix.com.au. The Configuration Sheet should be retained with a record of which machine has been allocated each username and password. A username and password should ONLY be allocated to ONE machine.

The following instructions detail how to install and configure a Windows 10 machine to use Cisco AnyConnect Secure Mobility Client over the Internet. Other operating system configurations should behave in a similar manner.

Cisco AnyConnect Secure Mobility Client needs to be installed on all PCs requiring access to Sunrise Exchange.

1. System Requirements

Verify that the computer meets these requirements to be able to install and run Cisco AnyConnect Secure Mobility Client:

The following information is sourced from the Cisco website:

- Supported Operating Systems: Windows 7, 8, 8.1 & 10
- Pentium class processor or greater
- 100 MB hard disk space
- Microsoft Installer, version 3.1
- Upgrading to Windows 8.1 from any previous Windows release requires you to uninstall AnyConnect, and reinstall it after your Windows upgrade is complete.
- Upgrading from Windows XP to any later Windows release requires a clean install since the Cisco AnyConnect Virtual Adaptor is not preserved during the upgrade. Manually uninstall AnyConnect, upgrade Windows, then reinstall AnyConnect manually or via WebLaunch.
- To start AnyConnect with Weblaunch, you must use the 32-bit version of Firefox 3.0+ and enable ActiveX or install Sun JRE1.4+
- ASDM version 7.02 or higher is required when using Windows 8 or 8.1

To install the VPN Client, an internet connection is required, along with Administrator privileges (depending upon local IT environment security)

Windows Vista/7 Home Basic and Windows Vista/7 Home Premium are not supported. AnyConnect does not work in a terminal server environment or on Windows Server operating systems.

2. Prior to Installing the VPN

For all connections to Sunrise™ Exchange, the following must be installed prior to downloading the Cisco AnyConnect Secure Mobility Client:

Latest Version of Java

Make sure the latest version of Java is installed on the system. This can be downloaded via http://java.com/en/download/inc/windows_upgrade_ie.jsp

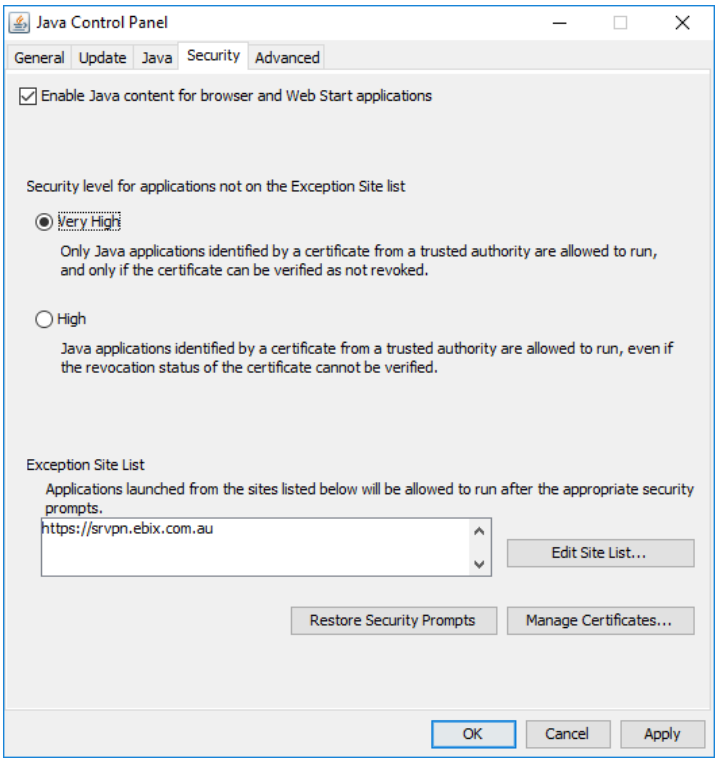
Java Settings

To allow the download of Cisco AnyConnect Secure Mobility Client, you will need to update your Java security settings.

The Java Console can be opened from the Start Menu. It is usually located at **Java > Configure Java**.

On the security tab, add the following to the Exception Site List, by clicking on **Edit Site List**, then **Add**.

https://srvpn.ebix.com.au

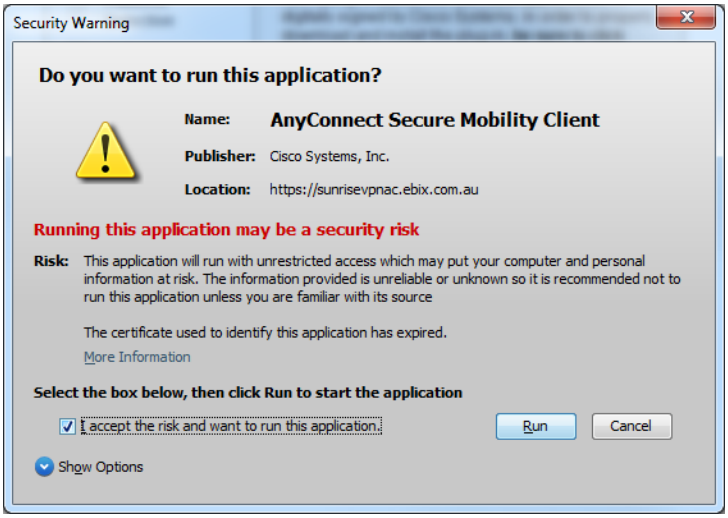


3. Downloading the software

To download the software for Cisco AnyConnect Secure Mobility Client, please use the latest ShareFile links provided in the email by Ebix support team.

The software will download and configure automatically.

If a Security Warning is displayed, tick the "I accept the risk and want to run this application" and click Run to continue

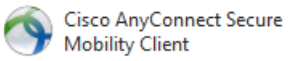


After successful connection to the Cisco AnyConnect Secure Mobility client, an icon will be displayed in the system tray  (near where the time is displayed, generally in the bottom right hand corner).

This indicates the connection is available and secure.

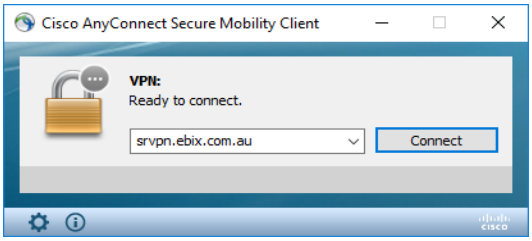
4. Connecting to Cisco AnyConnect Secure Client

When you first log into your PC, you will need to start the Cisco AnyConnect Security Mobility Client by navigating to **Programs** and selecting



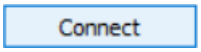
Right click to pin this program to your Taskbar for easy access.

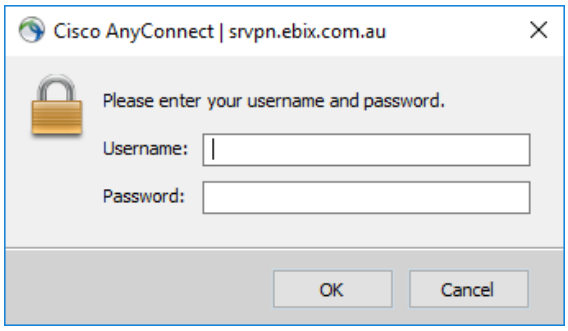
The Cisco AnyConnect Security Mobility Client connection window will be displayed:

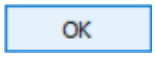


The URL will normally be completed for you, but if the field is blank please enter **srvpn.ebix.com.au**

Once the VPN has been accessed on a given day, you can simply navigate to the system tray and click the Cisco AnyConnect icon 

Click 



Enter your Username and Password and click 

You will need to re-enter your password each time you connect to the Cisco AnyConnect Security Mobility Client.

Passwords are an important part of computer security. Ebix recommend extreme vigilance in how you store this information, and take no responsibility for lost or stolen passwords. For any security concerns, please contact support@ebix.com.au.

After the VPN connection is established successfully, a padlock icon  will display in the System Tray on the desktop (near where the time is displayed, generally in the bottom right hand corner). This indicates the connection is available and secure.

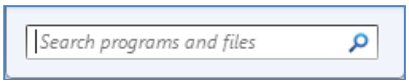
5. Confirming VPN Access

Ping Test

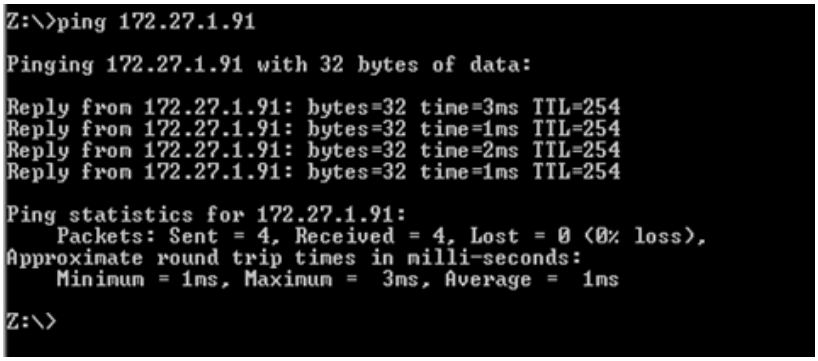
To confirm that VPN Access is working correctly:

Open a command prompt.

Click  .



Type **cmd** and select 'enter'.



Type **ping 172.27.1.91** and hit Enter.

If four lines beginning with **Reply from...** displays on the screen, this indicates the VPN is responding and the test has been successful.

To perform a basic test to check access to web-based Insurer products, perform the same test above, typing **ping 10.125.80.254**.

Again, if four lines beginning with **Reply from...** displays on the screen, this indicates access to web-based insurer products may be possible.

Last updated: 4 September 2024 12:16 PM

