

# Cisco Anyconnect Secure Mobility Client

1. Требования.
2. Где взять Cisco Anyconnect Secure Mobility Client.
3. Установка Cisco Anyconnect Secure Mobility Client.
4. Создание нового подключения.
5. Диагностика и устранение проблем при установлении подключения.
6. Контакты.

## Требования

- 1) Cisco Anyconnect Secure Mobility Client версии 3 совместим с ОС:
  - Windows 7, Vista, and XP,
  - Mac OS 10.5, 10.6 and 10.7,
  - Red Hat Enterprise Linux 5 Desktop,
  - Ubuntu 9.x.
- 2) Cisco Anyconnect Secure Mobility Client версии 4 **не совместим** с ОС:
  - Windows Vista and XP,
  - Mac OS X 10.6,
  - Ubuntu 9, 10, 11,
  - RHEL 5.x,
  - Все 32-битные версии ОС Linux.

Подробнее о совместимости

[http://www.cisco.com/c/en/us/td/docs/security/vpn\\_client/anyconnect/anyconnect40/release/notes/b\\_Release\\_Notes\\_AnyConnect\\_4\\_0.html](http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/release/notes/b_Release_Notes_AnyConnect_4_0.html)

Также есть вероятность, что Cisco Anyconnect Secure Mobility Client может не работать в ОС Windows 8.1.

Существуют приложения с функционалом Cisco Anyconnect Secure Mobility Client для ОС Android (**AnyConnect ICS+**) и Apple iOS(**Cisco Anyconnect**) , которые позволяют получить VPN-доступ и работать на мобильных устройствах, таких как мобильные телефоны и планшеты.

Приложения доступны по ссылкам:

Android <https://play.google.com/store/apps/details?id=com.cisco.anyconnect.vpn.android.avf>

iOS <https://itunes.apple.com/ru/app/cisco-anyconnect/id392790924?mt=8>

- 3) Для установки Cisco Anyconnect Secure Mobility Client необходимо иметь права администратора.

4) Для работы Cisco Anyconnect Secure Mobility Client использует порт TCP 443, соответственно, в Вашем сетевом экране должно быть правило, разрешающее исходящий трафик на порт TCP 443, а также входящий трафик с 443 порта TCP от сервера.

### **Где взять**

Файл для установки Cisco Anyconnect Secure Mobility Client доступен для загрузки на официальном сайте компании Cisco Systems по ссылке <https://software.cisco.com/download/navigator.html?mdfid=281268793&i=rm>

Внимание, для загрузки потребуется действующий сервис-контакт.

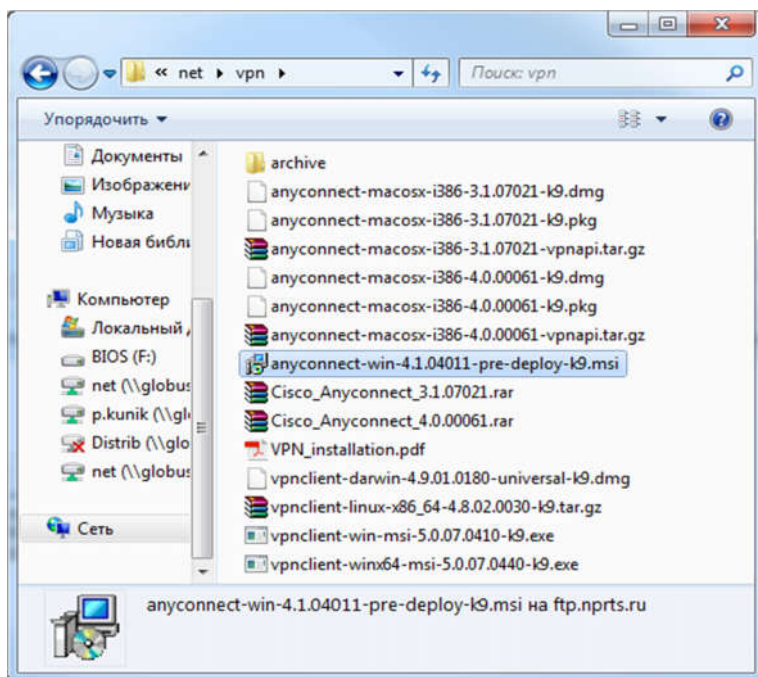
Также можно взять с ftp-сервера НПРТС по ссылке

<ftp://ftp.nprts.ru/net/vpn/>

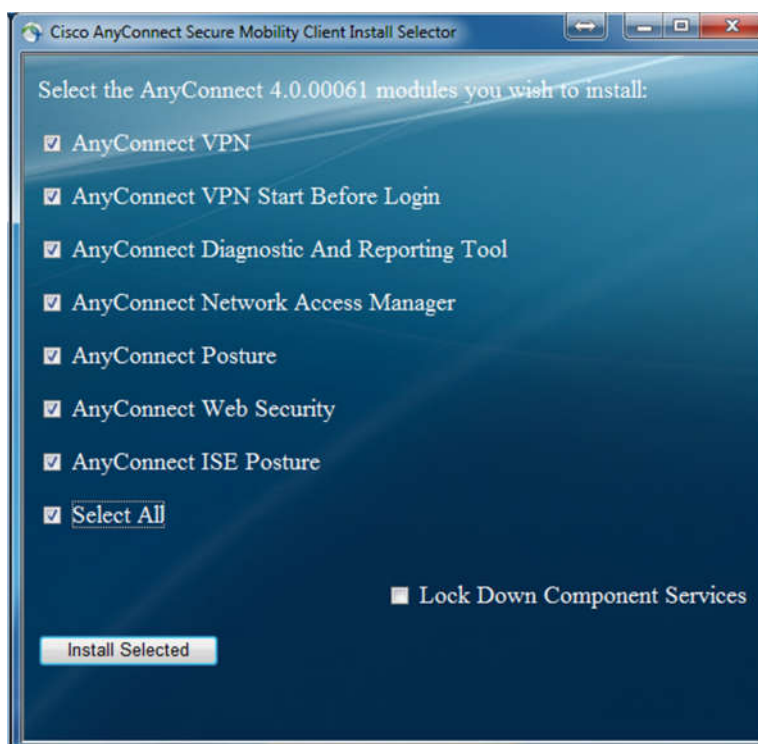
Рекомендуется использовать последнюю версию программы в том случае, если Вы не планируете установку клиента на неподдерживаемые Cisco Anyconnect Secure Mobility Client версии 4 операционные системы, например, Windows XP или Vista.

# Установка Cisco Anyconnect Secure Mobility Client в ОС Windows 7

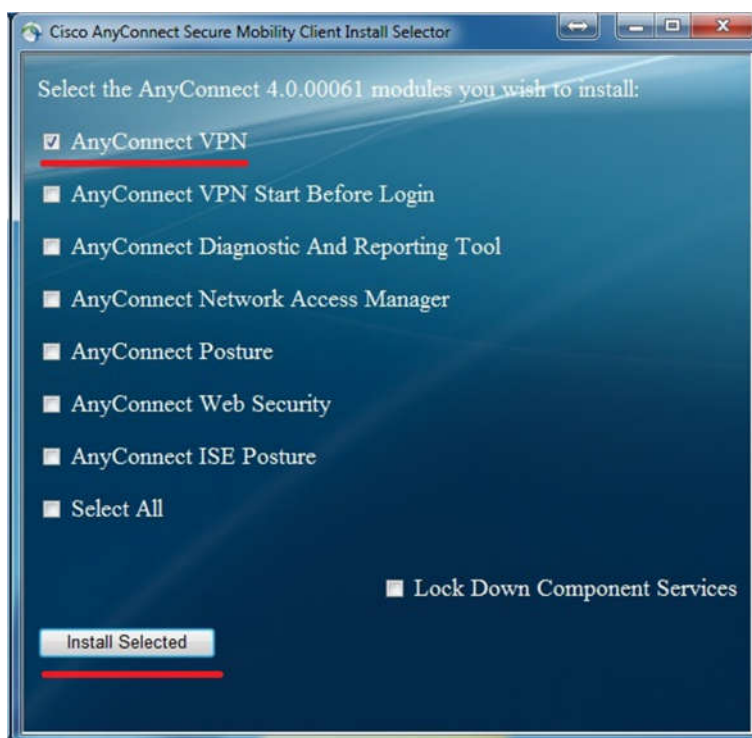
Нужно скачать с ftp-сервера <ftp://ftp.nprts.ru/net/vpn/> и запустить файл **anyconnect-win-4.1.04011-pre-deploy-k9.msi**



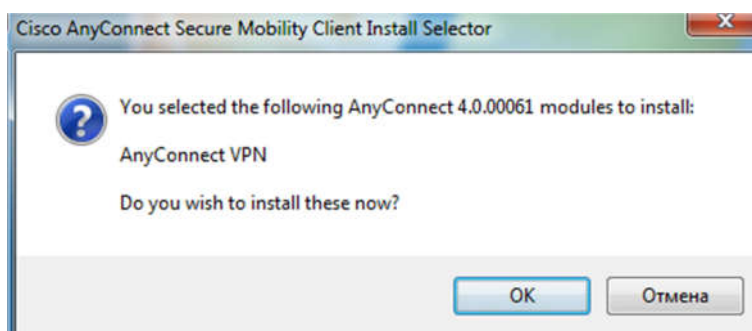
После запуска **Setup.exe** появится окно следующего вида:



Необходимо снять все галки, кроме верхней (**AnyConnect VPN**) и нажать кнопку **Install Selected**



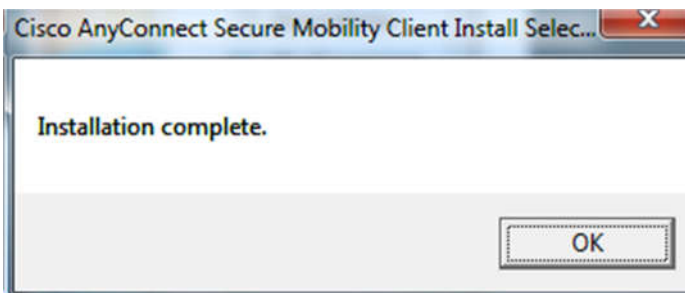
Далее надо подтвердить установку, нажав **ОК**:



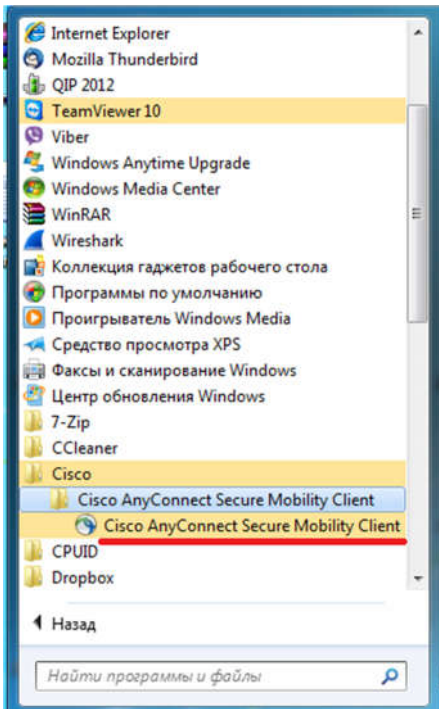
Нужно согласиться с лицензионным соглашением, нажав кнопку **Accept**:



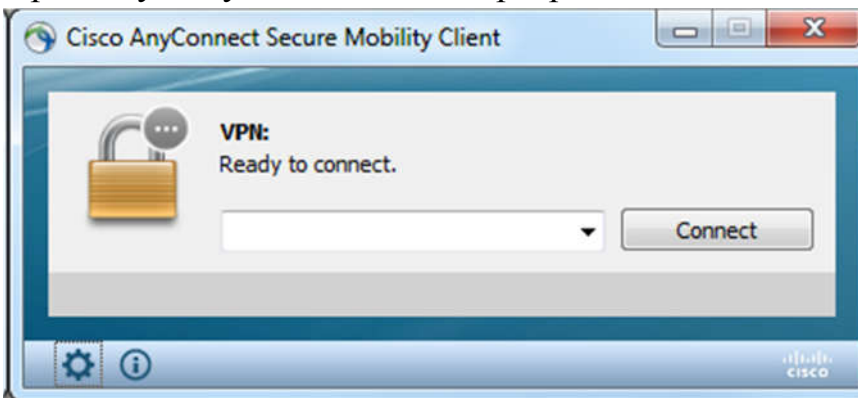
Установка запустилась, нужно подождать сообщения об окончании установки, а затем нажать **ОК**.



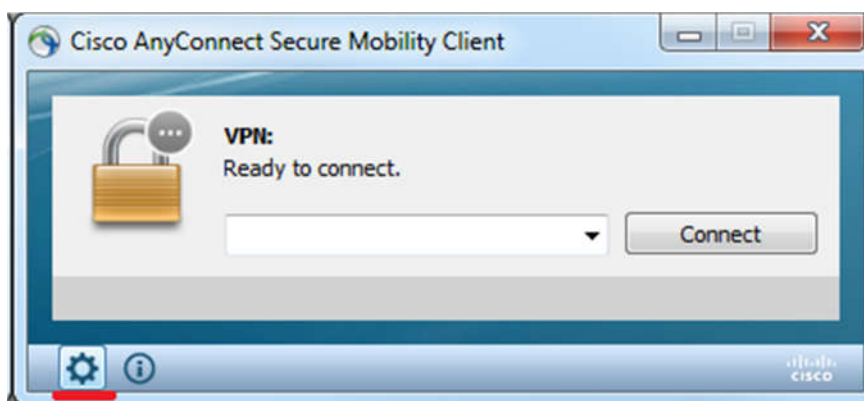
Ярлык клиента в ОС Windows можно найти, зайдя в меню **Пуск**, нажав **Все программы** и открыв папку **Cisco**. Ярлык для удобства запуска можно скопировать на рабочий стол.



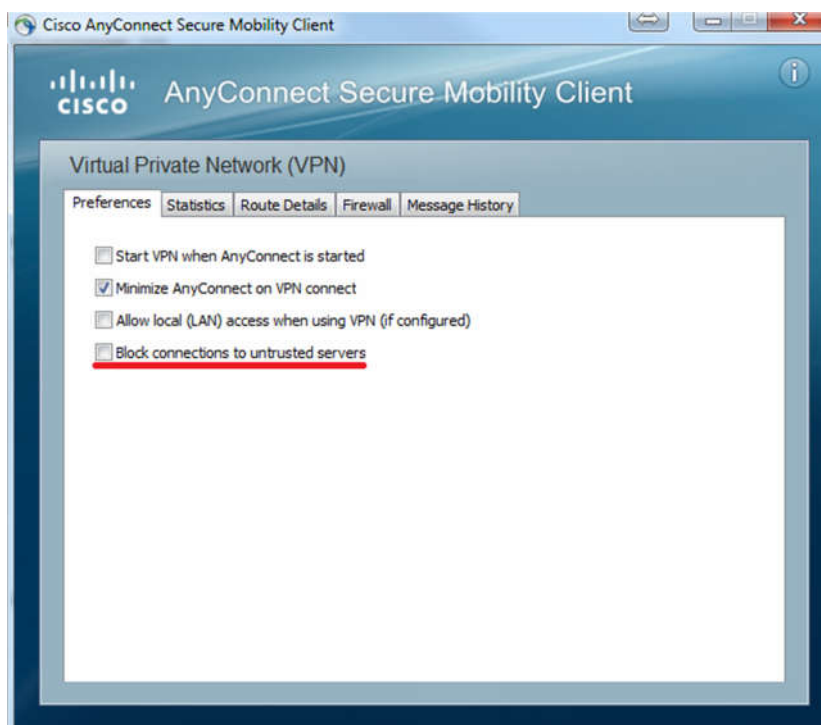
При запуске установленной программы появляется окно следующего вида:



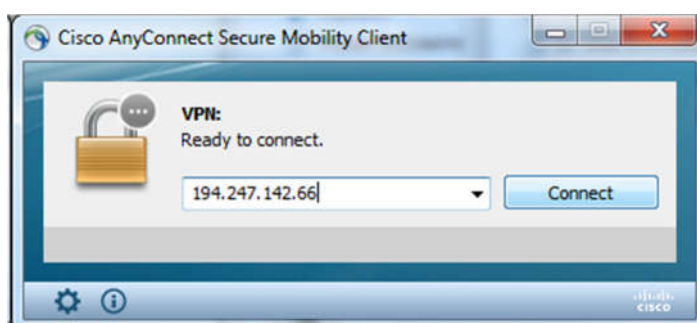
При первом запуске следует выполнить настройку. Для этого надо нажать кнопку со значком шестерёнки:



Далее нужно открыть вкладку **Preferences** и снять галочку **Block connections to untrusted servers**, которая установлена по умолчанию. Галочка должна быть снята!



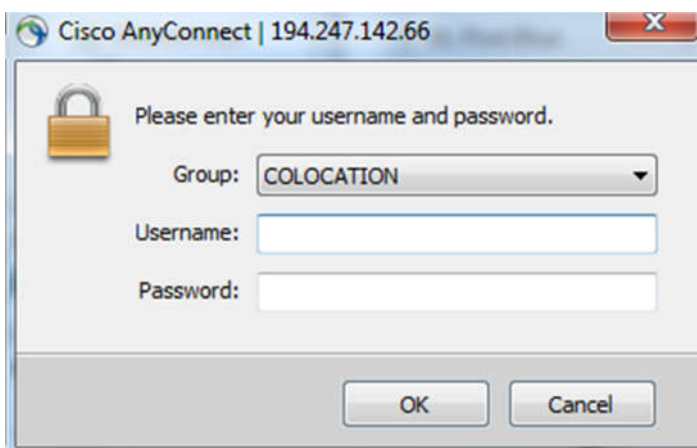
После этого нужно вписать поле окна IP-адрес VPN-сервера **194.247.142.66** и нажать **Connect**



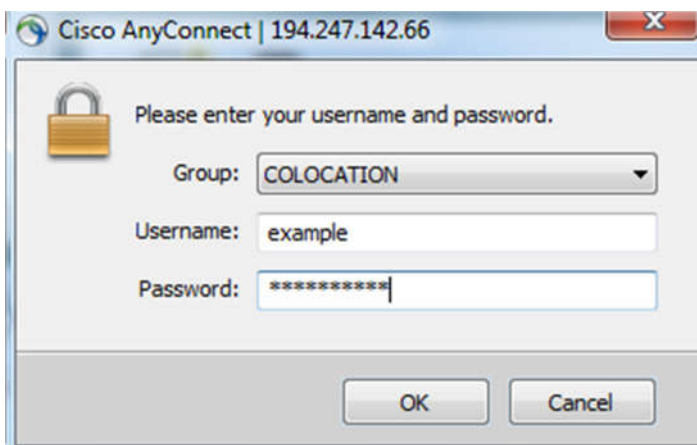
Появляется предупреждение, нажимаем **Connect Anyway**



Появляется окно авторизации.

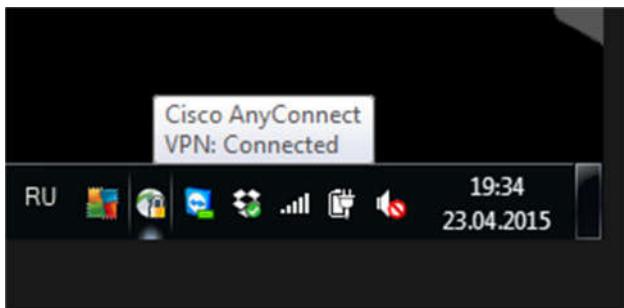


Выбираем группу **OFFICE** (для сотрудников) или **COLOCATION** (для клиентов-колокаторов), заполняем поля **Username** (логин) и **Password** (пароль). Данные были высланы Вам в письме по электронной почте при регистрации логина. После ввода данных нажимаем **OK**.

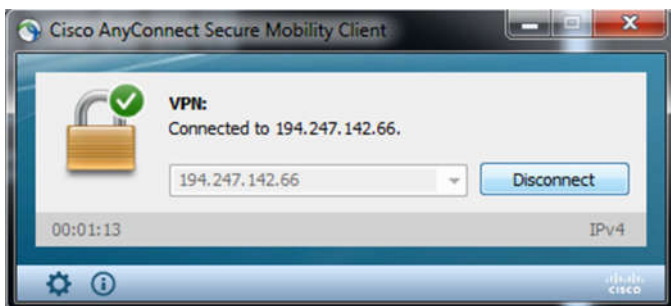




После установки в области уведомлений в нижнем правом углу экрана появляется значок в виде круга с закрытым замком. При наведении курсора появляется надпись, что соединение установлено.



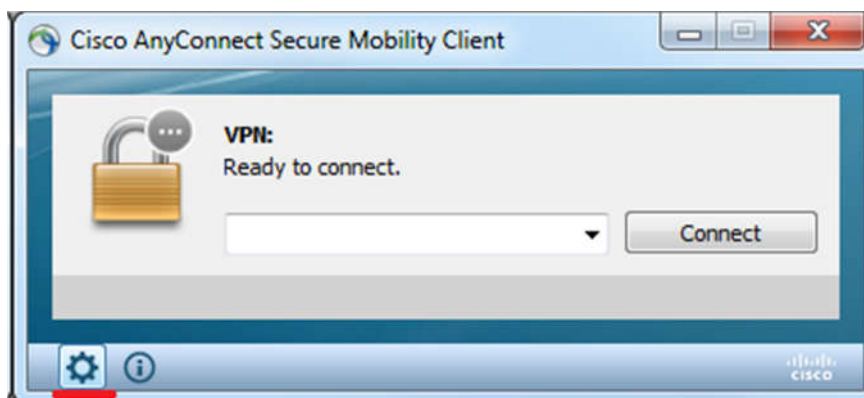
При нажатии мышью появляется окно клиента. Отключиться от VPN-сервера можно, нажав кнопку **Disconnect**



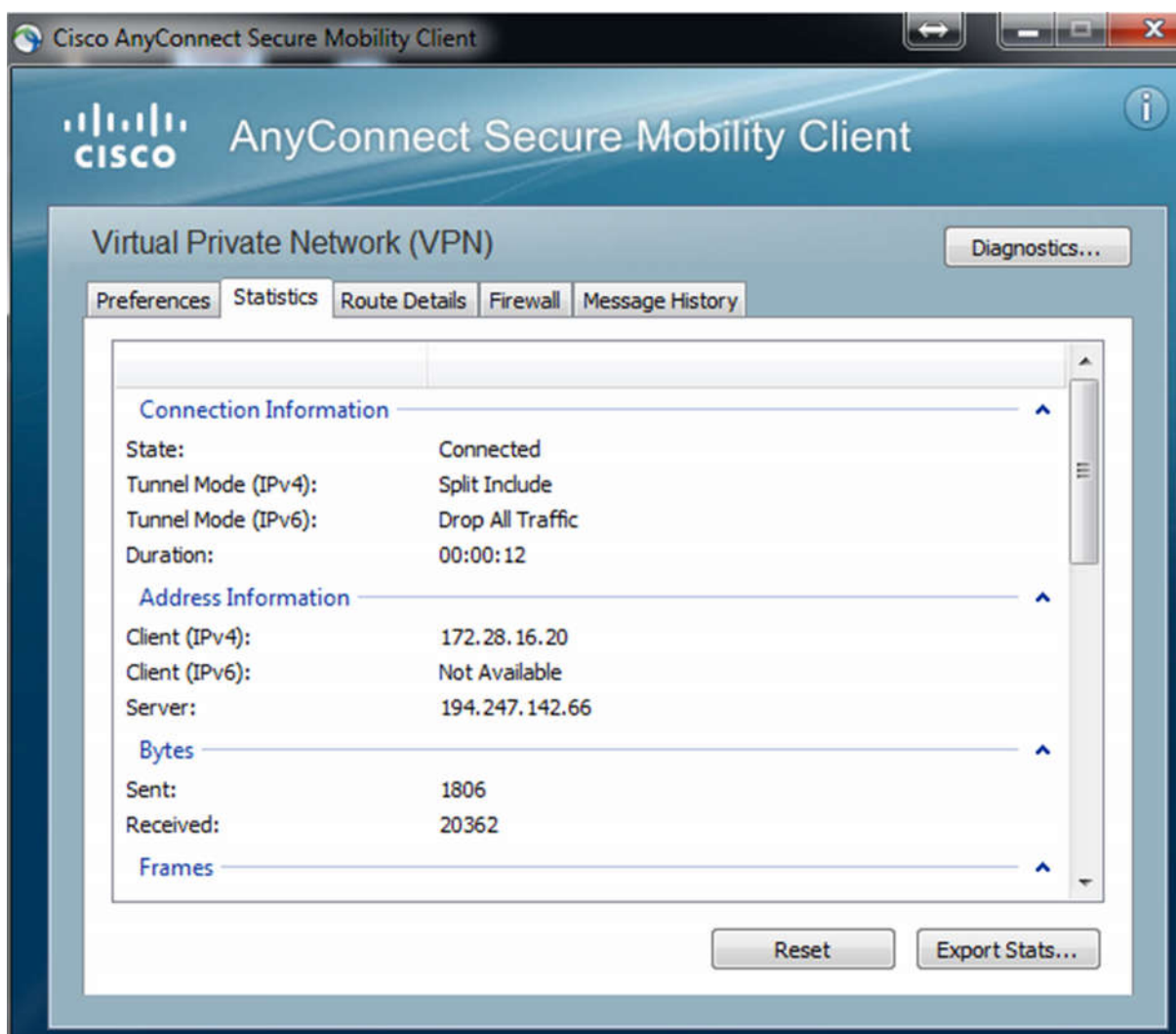
## Диагностика

В случае если подключение не устанавливается, не работает или ведёт себя странно, можно изучить содержимое вкладок **Statistics** и **Message History**.

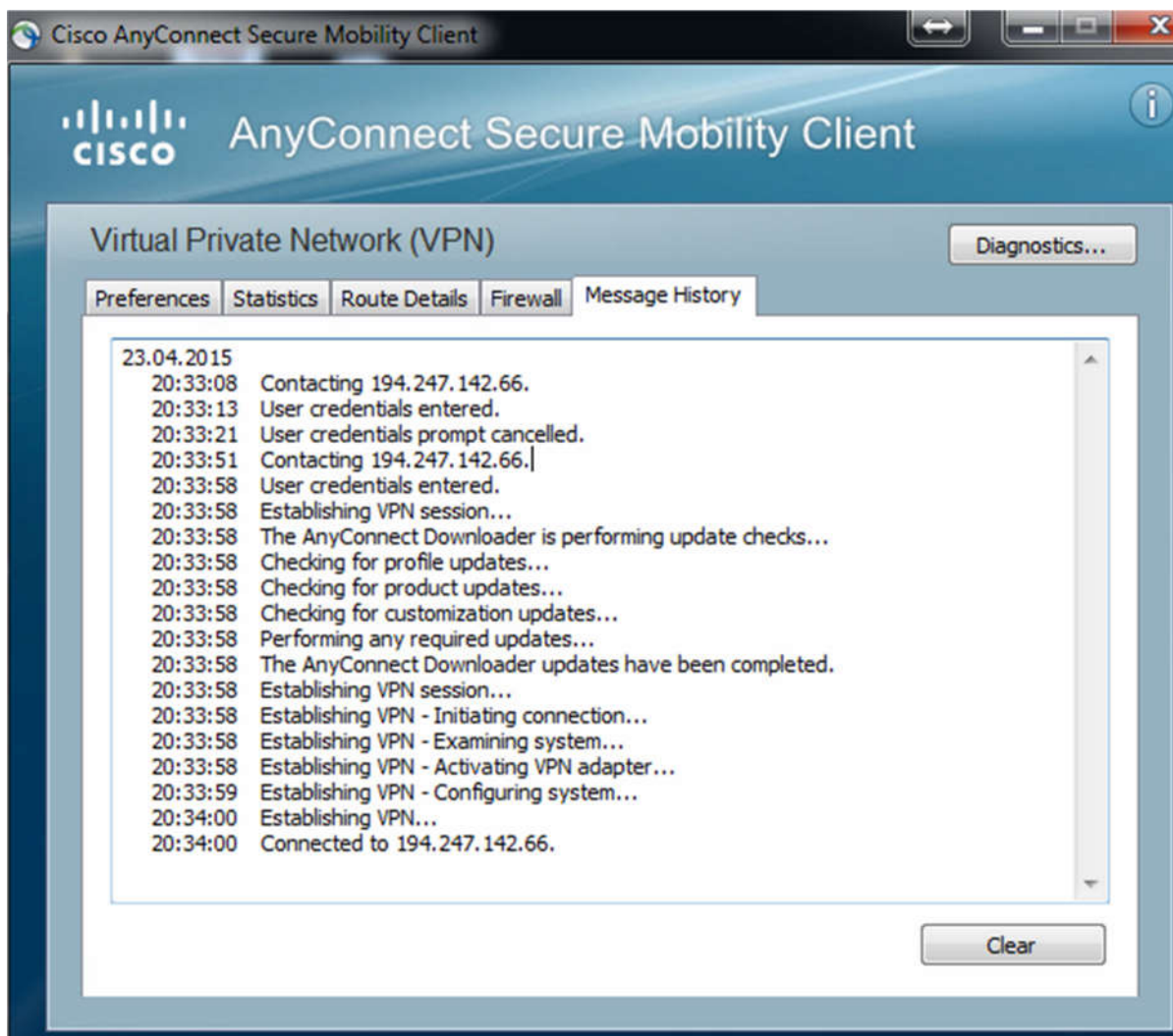
Для этого нужно нажать на кнопку с изображением шестерёнки:



Вкладка **Statistics** содержит информацию о состоянии туннеля, статистику и ip-адрес виртуального туннельного адаптера.



Вкладка **Message History** содержит лог подключения, а именно – что произошло и когда произошло.



Помимо этого, для диагностики в ОС Windows можно воспользоваться следующими командами:

**ipconfig /all** – выводит информацию по всем сетевым адаптерам ОС.

**route print** – выводит таблицу маршрутизации ОС.

## **Контакты**

[net@rts.ru](mailto:net@rts.ru) – по вопросам сетевого подключения.

[sales@nprts.ru](mailto:sales@nprts.ru) – по вопросам приобретения и оплаты услуг.

Телефон: +7 (495) 705-90-31