

SSL VPN for Gen 3



[Home](#) > [SSL VPN for Gen 3](#)



This article is for Generation 3 (Gen 3) users.

Download and install the SSL VPN client

The Cisco AnyConnect Client is used to create a secure connection from your local computer to your Secure Cloud Servers within Armor's environment.

1. Download the client. Select the link that corresponds to your operating system:
 - Windows
 - <https://get.core.armor.com/extra/anyconnect/anyconnect-win-4.7.02036-core-vpn-predeploy-k9.msi>
 - Mac OSX
 - <https://get.core.armor.com/extra/anyconnect/anyconnect-macos-4.7.02036-predeploy-k9.dmg>
 - Linux
 - <https://get.core.armor.com/extra/anyconnect/anyconnect-linux64-4.7.02036-predeploy-k9.tar.gz>
2. Once the file has downloaded, run the installer, and then follow the on-screen prompt.
3. If you have any issues downloading or installing the AnyConnect client, please contact Armor Support through the [Armor Ticketing System](#).

Connect to the SSL VPN client

1. In your local machine, open the **Cisco AnyConnect Client**.
2. Verify and select the correct hostname:

Data center	Web address
Dallas	vpn-1.armor.com
Phoenix	vpn-6.armor.com
London	vpn-3.armor.com
Amsterdam	vpn-4.armor.com
Singapore	vpn-8.armor.com

3. Enter your VPN credentials.
4. Click **Connect**.
 - If you have enabled two-factor authentication for your account, then answer the phone call from Armor, and then follow the instructions.
 - If you need to reset your password, please contact Armor Support through the [Armor Ticketing System](#).

Manage SSL VPN accounts

To add, remove, or modify your Gen 3 SSL VPN account please contact Armor Support through the [Armor Ticketing System](#).

Related documentation

- [SSL VPN](#) (for Gen 4 users)