

SSL VPN

Armor Knowledge Base

Topics Discussed

- [Enable, Download, and Install Your SSL VPN Access \(Account Administrators\)](#)
- [Download and Install Your SSL VPN \(Non-Account Administrators\)](#)
- [Disable SSL VPN for your user](#)
- [View user activity for SSL VPN](#)



Armor offers one free SSL VPN user per account.



To fully use this screen, you must have the following permissions assigned to your account:

- Write SSL VPN Devices and Users
- Read SSL VPN Devices and Users
- Read Virtual Data Centers

Enable, Download, and Install Your SSL VPN Access (Account Administrators)



If you have created a virtual machine, then you must enable and install your SSL VPN client.



These instructions apply to account administrators.



If you have the **Continuous Server Replication (Disaster Recovery)** add-on product in your account, then you must download the SSL VPN client for the appropriate live recovery environment.

- If your primary environment is **DFW01**, then you should download the client for **PHX01-Recovery** environment.
- If your primary environment is **PHX01**, then you should download the client for **DFW01-Recovery** environment.



If you run Ubuntu 16.x, then please review [Install SSL VPN for Ubuntu 16.x](#).

If you run Ubuntu 18.x, then please review [Install SSL VPN for Ubuntu 18.x](#).

If you run Mac OS 10.11 or higher, then please review [Install SSL VPN for Mac OS 10.11+](#).



For Account Administrators only.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **SSL VPN**.
3. Click **Members**.
4. Click the plus (+) icon.
5. In the field, enter and select the name of the user, or their email address.
6. Mark the desired data center or data centers that the user can connect to.
7. Click **Submit**.
 - The newly added user will appear in the table; the table is organized in alphabetical order, based on the first name of the user.
8. Click **Client**.
9. Click **Download SSL VPN client**.
 - AMP will automatically detect your operating system; however, you can click **Download for another platform** to view other operating system options.
 - When you open the client, follow the on-screen installation instructions.



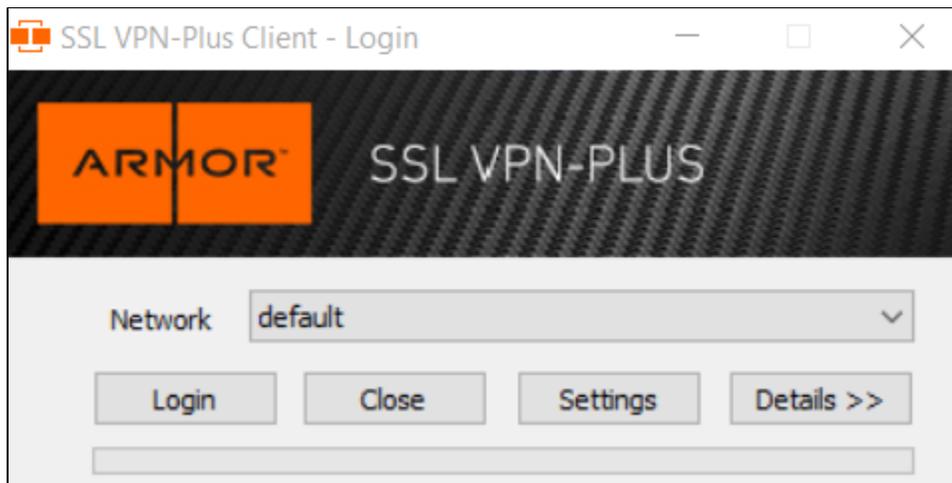
- For **Windows** users, the client will download as a **.zip** file.
 - Extract the installation files to your local hard drive.
 - Launch the **installer.exe** file to begin the installation.



- For **Mac OS** users, the client will download as a **.tgz** file.
 - Extract the installation files to your local hard drive.
 - Access the **mac_phat_client** folder, and then run the **naclient.pkg** installer.
 - When you run the installer, you will see an error regarding the certificate. Click **Continue**. (In a future release, Armor will resolve the issue.)
 - To launch the SSL VPN client, in your **Applications** folder, search for **naclient**.
 - If you run Mac OS 10.11 or higher, then please review [Install SSL VPN Client for Mac OS, version 10.11 and higher](#).

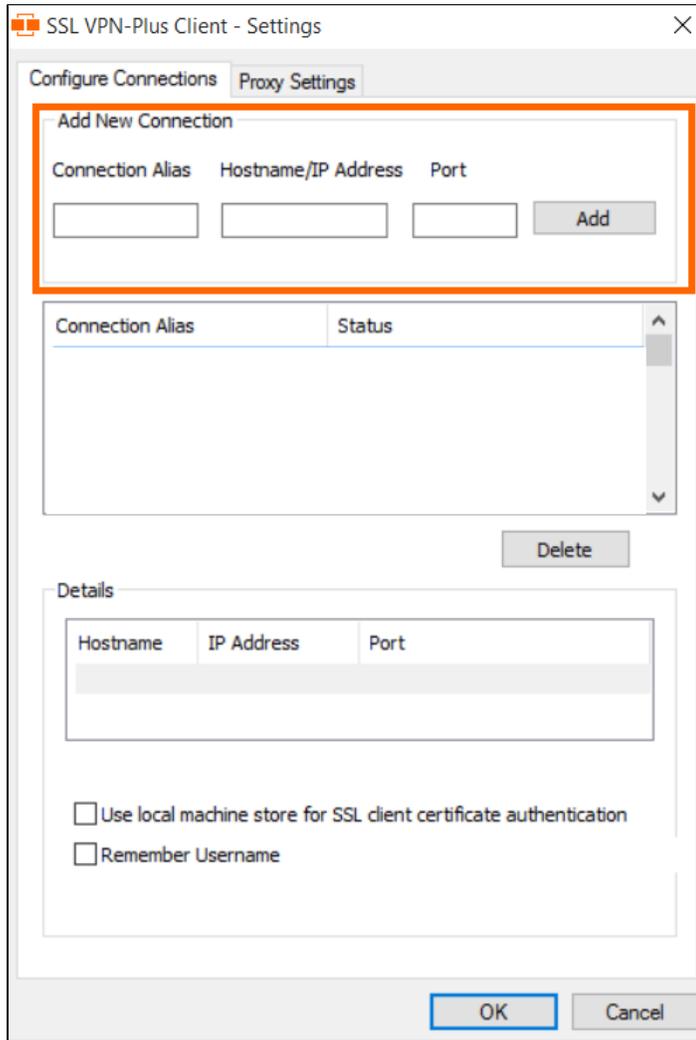
10. After installation, open the client.

- In the drop-down menu, **default** will be listed.

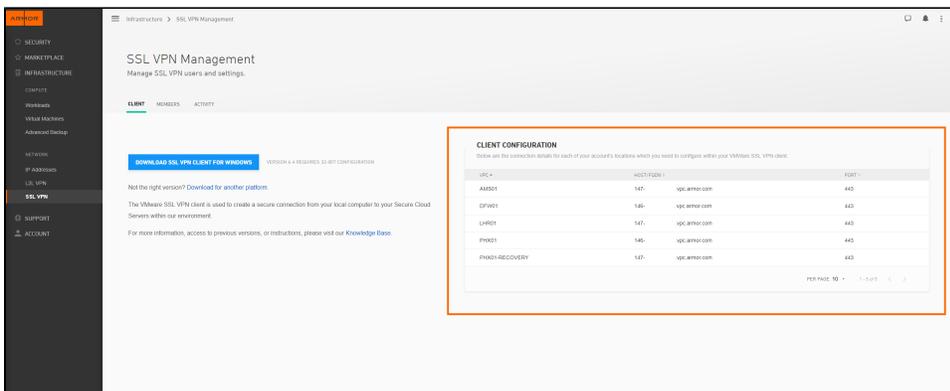


11. Click **Settings**.

- To add a new connection, you must enter a **Connection Alias**, **Hostname/IP Address**, and **Port**, which you can find in AMP.



12. Return to AMP, specifically to the **Client** section of the **SSL VPN** screen.
13. Use the **Client Configuration** table to locate the data center and corresponding information to add to the client.



14. Under **Client Configuration**, copy the **Location** information, and then paste that information into **Connection Alias**.
15. Under **Client Configuration**, copy the **HOST/FQDN** information, and then paste that information into **Hostname/IP Address**.
16. Under **Client Configuration**, copy the **Port** information, and then paste that information into **Port**.
17. Click **Add**.
18. Click **OK**.
19. In the drop-down menu, select the newly created connection.
20. Log into the client.
 - Your SSL VPN login credentials are the same credentials you use to access the Armor Management Portal (AMP).

Download and Install Your SSL VPN (Non-Account Administrators)



These instructions apply to non-account administrators.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **SSL VPN**.
3. Click **Members**.
4. Click the plus (+) icon.
5. In the field, enter and select the name of the user, or their email address.
6. Mark the desired data center or data centers that the user can connect to.
7. Click **Submit**.
 - The newly added user will appear in the table; the table is organized in alphabetical order, based on the first name of the user.
8. Click **Client**.
9. Click **Download SSL VPN client**.
 - AMP will automatically detect your operating system; however, you can click **Download for another platform** to view other operating system options.
 - When you open the client, follow the on-screen installation instructions.

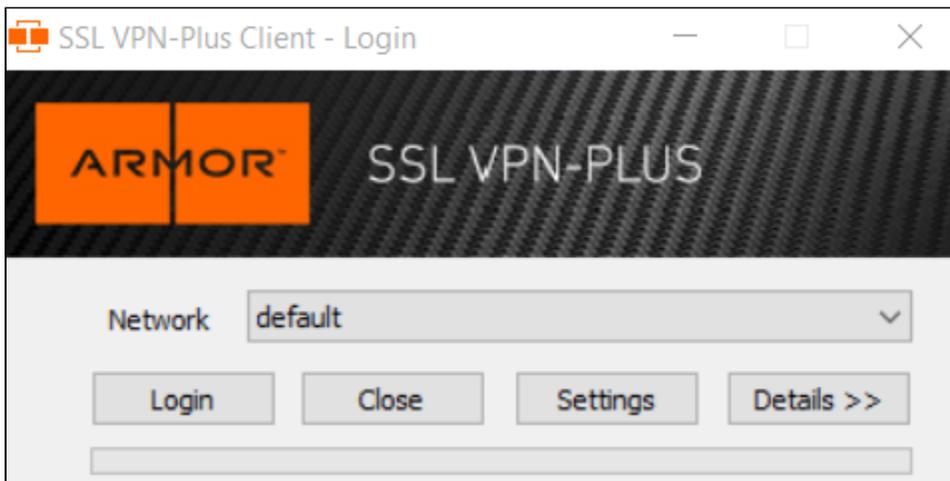


- For **Windows** users, the client will download as a **.zip** file.
 - Extract the installation files to your local hard drive.
 - Launch the **installer.exe** file to begin the installation.

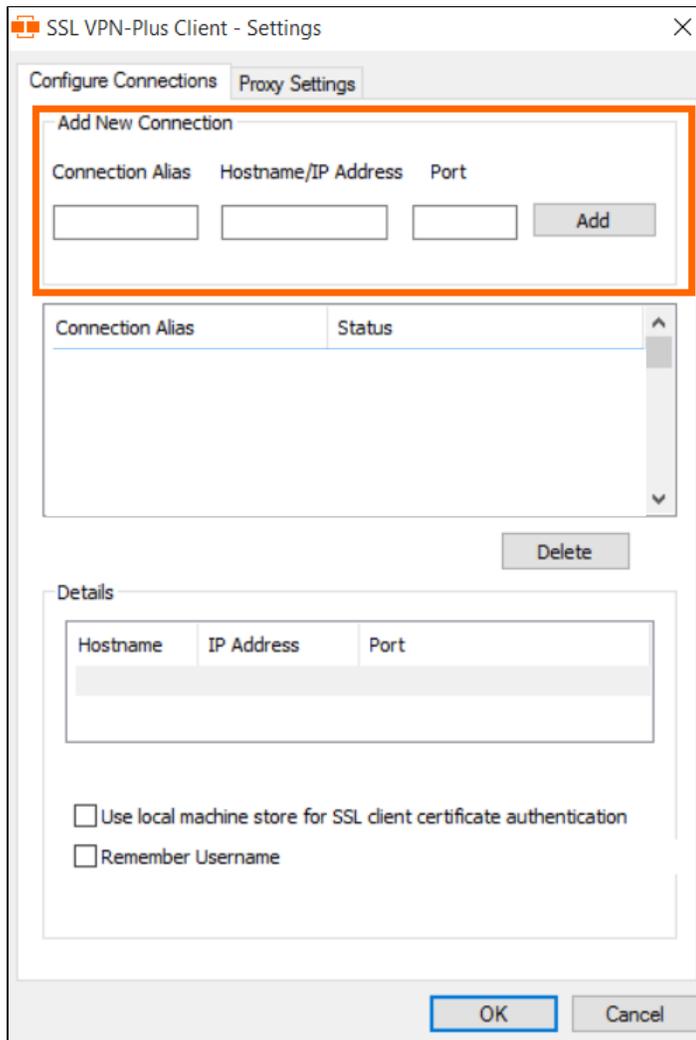


- For **Mac OS** users, the client will download as a **.tgz** file.
 - Extract the installation files to your local hard drive.
 - Access the **mac_phat_client** folder, and then run the **naclient.pkg** installer.
 - When you run the installer, you will see an error regarding the certificate. Click **Continue**. (In a future release, Armor will resolve the issue.)
 - To launch the SSL VPN client, in your **Applications** folder, search for **naclient**.
 - If you run Mac OS 10.11 or higher, then please review [Install SSL VPN Client for Mac OS, version 10.11 and higher](#).

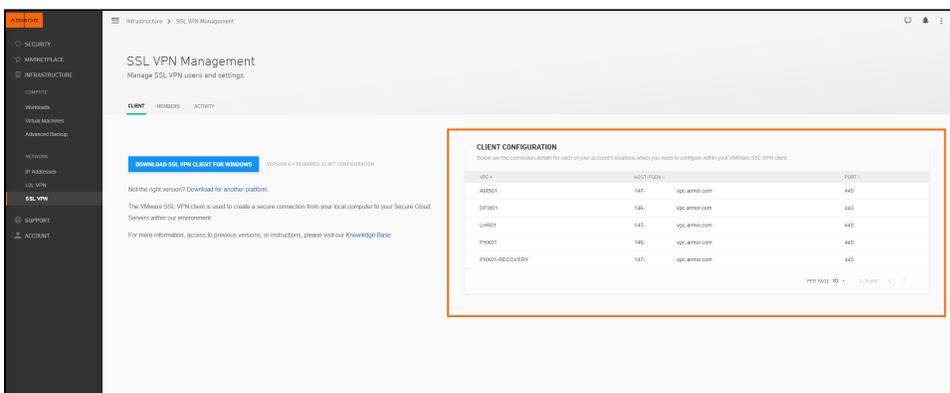
10. After installation, open the client.
 - In the drop-down menu, **default** will be listed.



11. Click **Settings**.
 - To add a new connection, you must enter a **Connection Alias**, **Hostname/IP Address**, and **Port**, which you can find in AMP.



12. Return to AMP, specifically to the **Client** section of the **SSL VPN** screen.
13. Use the **Client Configuration** table to locate the data center and corresponding information to add to the client.



14. Under **Client Configuration**, copy the **Location** information, and then paste that information into **Connection Alias**.
15. Under **Client Configuration**, copy the **HOST/FQDN** information, and then paste that information into **Hostname/IP Address**.
16. Under **Client Configuration**, copy the **Port** information, and then paste that information into **Port**.
17. Click **Add**.
18. Click **OK**.
19. In the drop-down menu, select the newly created connection.
20. Log into the client.
 - Your SSL VPN login credentials are the same credentials you use to access the Armor Management Portal (AMP).

Disable SSL VPN for your user



These instructions apply to account administrators.



To disable SSL VPN for a user, you must have the following permissions assigned to your account:

- Write SSL VPN Devices and Users
- Read SSL VPN Devices and Users
- Read Virtual Data Centers

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **SSL VPN**.
3. Click **Members**.
4. In the top bar, select the desired data center.
5. Locate and hover over the desired user.
6. Click the trash icon that appears.
7. Click **Remove Access**.

View user activity for SSL VPN

You can use these instructions to view how your users have interacted with their SSL VPN device.



To view user activity for SSL VPN users, you must have the following permissions assigned to your account:

- Write SSL VPN Devices and Users
- Read SSL VPN Devices and Users
- Read Virtual Data Centers

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **SSL VPN**.
3. Click **Activity**.

Column	Description
Date	This column displays the date and time that the user interacted with their SSL VPN device.
User Name	This column displays the email address of the user. <div data-bbox="337 1285 1263 1369"> In some cases, you may see unknown user listed. The third-party vendor is aware of this bug.</div>
Source IP Address	This column displays the user's IP address where the authentication took place.
Local IP Address	This column displays Armor's connection source.



Troubleshooting

If you are concerned about your billing statement for SSL VPN devices (members), consider that:

- You may have members in other data centers. In the top menu, there is a drop-down menu that you can use to switch across different data center views. As a result, when you switch to a different data center view, you may see additional members.
- If you have the same SSL VPN member in multiple data centers, you will only be billed for the one member. For example, if you have one member in DFW01 and the same member in LHR01, then you will only be billed for one member; however, if you have multiple members in a single data center location, then you will be charged for those additional members.
 - In short, you will be billed for every unique member, regardless of how many data centers are included.



Was this helpful?

*

Your Rating: 

Results:  4 rates