Invited Users

For invited users:

Before your account was created, your account administrator decided the proper roles and permissions for your account.

Consult with your account administrator to understand what permissions you have and how you should configure your account.

You can use this document to complete the account signup process and review high-level action items to complete.

1. In the email from Armor, click the link.
    - You will be redirected to enter your account security information.

In this step, you will add your phone number to your account. This phone number will be used for multi-factor authentication. To complete the account signup process and to log into AMP, you must be near this phone number.

1. Note your Armor username.
    - The **Username** will be pre-populated with the email address of the **Primary Contact** for the account.
2. In **Password** and **Confirm Password,** create and enter an account password.
    - Your password must be at least 12 characters in length.
    - Your password must contain an upper-case character, a lower-case character, a number, and a special character.
    - Your password cannot contain personal information, such as your name, email address, birthday, etc. For example, if your name is John Smith, then you cannot use joh or smi in your password.
    - You can only change your password once every 24 hours.
    - Passwords expire after 60 days.
    - After 6 failed login attempts, you will be locked out of your account for an hour. To resolve this, you must contact your account administrator or contact Armor Support.
    - After 15 minutes of no activity, you will be logged out of the Armor Management Portal (AMP).
3. Complete the **Challenge Phrase** and **Challenge Response**.
    - If you call Armor for technical support, you will be asked the **Challenge Phrase**, and you must correctly answer the **Challenge Response**.
    - Do not use inappropriate language or suggestive material.
    - The answer must be at least five characters long.
4. In **Phone Number,** select your country code / flag, and then enter your phone number.
    - This phone number will be used for multi-factor authentication (MFA). Every time you log into the Armor Management Portal (AMP), you will receive a phone call in order to complete the login process.
    - You can enter a phone number with spaces and special characters, such as (555) 555-555.
    - (Optional) If your phone number contains an extension, enter the number in **Extension**. You cannot include spaces or special characters in this field.
5. Click **Validate** to validate the phone number entered.
    - You will receive a phone call; answer the phone, and then follow the instructions.
    - (Optional) After you complete the signup process, you can configure your account to use the Microsoft Authenticator application for MFA. To learn how to use this application, see Configure multi-factor authentication for your account.
6. Click **Continue**.
    - You will be redirected to the Armor Management Portal (AMP) login screen.

Workloads and **tiers** are visual tools used in the Armor Management Portal (AMP) to help you organize your virtual machines and corresponding resources. Workload refers to a container of virtual machines that live inside the Armor data center. Tiers are levels within workloads.

1. In the Armor Management Portal, in the left-side navigation, click **Infrastructure**.
2. Click **Virtual Machines**.
3. Hover over the plus (+) icon, and then click the **Virtual Machine** icon.
    - If you do not have any virtual machines listed, then click **Deploy New**, and then select **Virtual Machine**.
4. Locate and select the desired operating system and operating system version.
5. On the right side, use the **Region** drop-down menu to select the data center to host your virtual machine.
6. Select the desired virtual machine based on your CPU and memory needs (GB).
    - You can click **High CPU** or **High Memory** to filter the list of virtual machines. You can also click **Show All Options** to see every virtual machine offering.
    - Armor labels virtual machines by CPU and memory features. For instance, **2x4** indicates that the virtual machine has 2 CPU and 4 GB of memory.
7. In **Name**, enter a descriptive name for your virtual machine.
8. In **Workload**, select **New Workload**.
9. In **New Workload Name**, enter a descriptive name.
10. In **New Tier Name**, enter a descriptive name.
11. In **Location**, select and verify the data center to host your virtual machine.
12. Under **Access Credentials**, note your username to access the virtual machine.
13. In **Password**, enter a secure password to use to access the virtual machine.
    - Your password must contain:

        - An upper-case letter
        - A lower-case letter
        - A number
        - A special character: ! @ # $ % ^ * ( ) { } [ ]
    - You can also click **Generate Password** to allow Armor to create a password.
14. (Optional) For additional storage, under **Storage Substrate** and **Disk Size**, select your desired storage, and then click **Add Disk**.
15. On the right-side menu, review the pricing information, and then click **Purchase**.
    - When you order a virtual machine, you are also ordering Intelligence Security Model (ISM) for the virtual machine. Prices for ISM will vary based on the number of virtual machines you have ordered. IMS pricing is based on the following tiered structure:

Tier	Number of Virtual Machines
1	1 - 10
2	11 - 25
3	26 - 100
4	101 - 250
5	251 - 500
6	500 +

16. To view the status of your newly created virtual machine, in the left-side navigation, click **Infrastructure**, click **Virtual Machines**, and then search for your newly created virtual machine.

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+.

Before you can download and install your SSL VPN, the account administrator must add the following permissions to your account:

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

Additionally, your account administrator must enable your account to download and install the client.

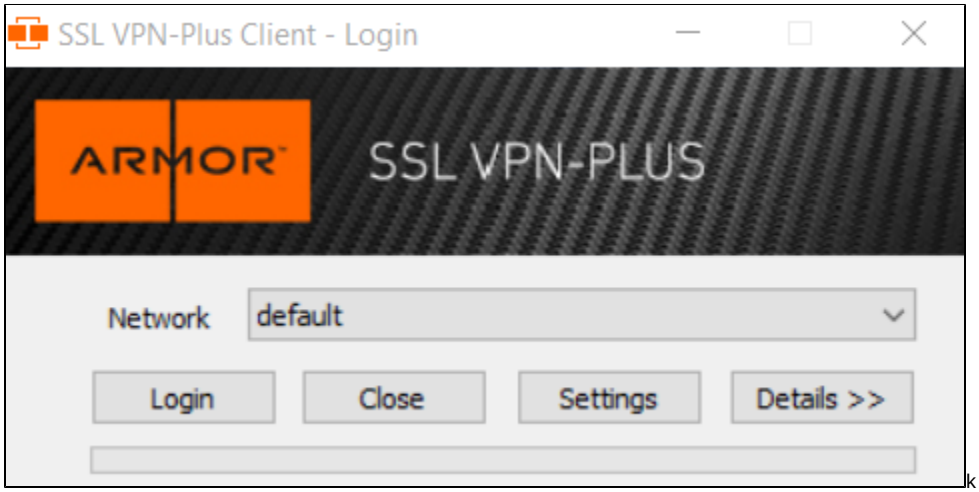
Confirm with your account administrator before you attempt to download and install.

This section is for Account Administrators only.

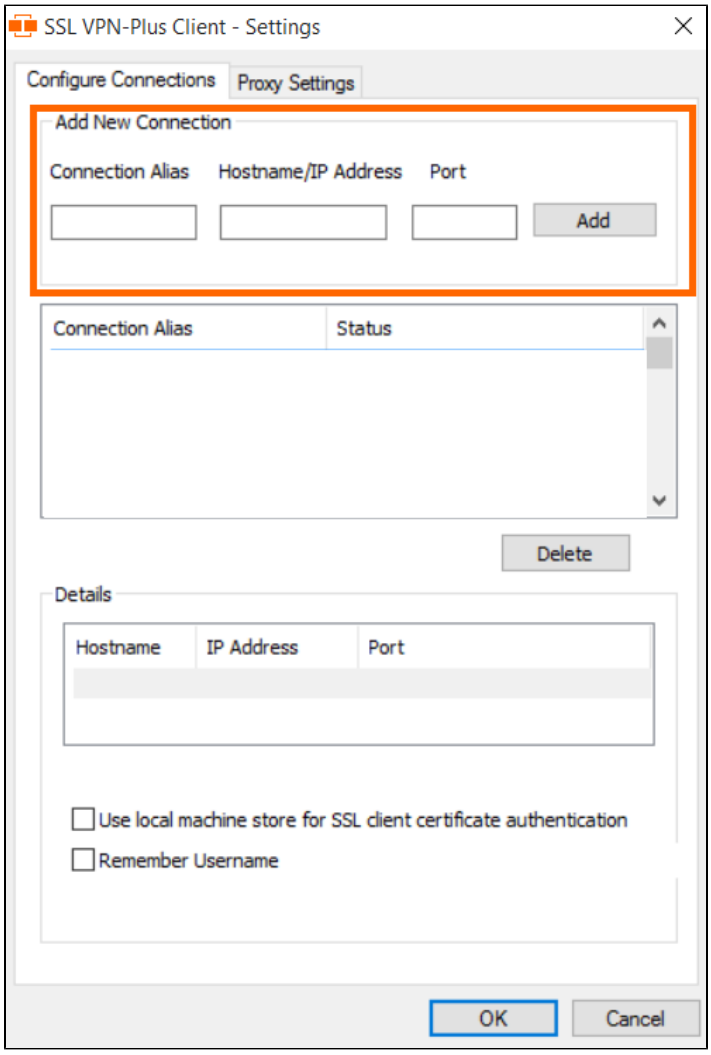
1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **SSL VPN**.
3. Click **Members**.
4. Click the plus (+) icon.
5. In the field, enter and select the name of the user, or their email address.
6. Mark the desired data center or data centers that 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.

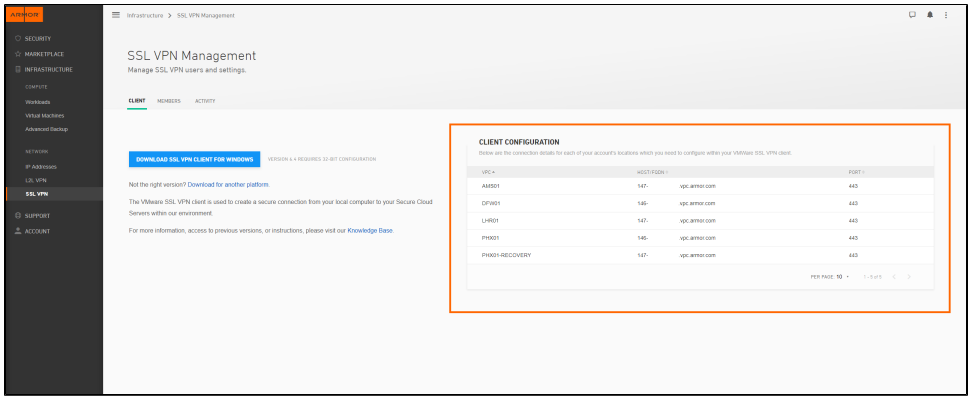
- In the drop-down menu, **default** will be listed.



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).

Step 1: Create an IP Group

In the **Firewall** screen, each entry in the table represents a single firewall rule; however, each firewall rule can contain several IP addresses or just a single IP address.

You can combine related IP addresses into a single **IP Group**. For example, if you want to block traffic from three separate IP address, you do not have to create three separate firewall rules. Instead, you can combine the three separate IP addresses into a single, configurable **IP Group**. Then, when you create a firewall rule, you can pick the newly created **IP Group** as your **Source** or **Destination** IP addresses.

1. In the Armor Management Portal (AMP), on the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top drop-down menu, select the desired data center.
4. Click **IP Groups**.
5. Click **Actions**, and then click **New Group**.
6. In **IP Group Name**, enter a descriptive name.
    - Armor recommends that you add **Source** or **Destination** into the name of the IP Group to help you identify the IP Group as the **Sour ce** or **Destination** IP group.
7. In **Add Members To Group**, enter a member, and then click the plus icon.
    - You can enter:
        - A single IP address
        - A range of IP addresses
        - CIDR
    - You must add at least one member.
    - You can add multiple members to a service group.
8. Click **Apply**.
    - The newly created IP group will appear at the bottom of the table.

Step 2: Create a Service Group

In the **Firewall** screen, each entry in the table represents a single firewall rule; however, each firewall rule can contain several protocols (and ports).

You can combine related protocols (and ports) into a **Service Group**. For example, if you want to create a firewall rule to block three types of traffic, you do not have to create three separate firewall rules. Instead, you can combine the three types of traffic (protocols and ports) into a single, configurable **Service Group**. Then, when you create a firewall rule, you can pick the newly created **Service Group**.

1. In the Armor Management Portal (AMP), on the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top drop-down menu, select the desired data center.
4. Click **Service Groups**.
5. Click **Actions**, and then click **New Group**.
6. In **Service Group Name**, enter a descriptive name.
7. In **Add Members To Group**, enter the service or sub-protocol, and then click the plus (+) icon.
    - You must add at least one member.
    - You can add multiple members to a service group.

Service or Sub-Protocol	Notes	Example
Services (TCP, UDP, etc.)	You must enter a port number. These services are not case-sensitive.	• tcp/80 • TCP/80 • Tcp/80

		• tCp/80
Additional services (AARP, AH, etc.)	These additional services are not case-sensitive. Do not enter a port number with these additional services.	• ATALK • igmp • Gre
Sub-protocols (echo-reply, redirect, etc.)	You must enter **icmp**, followed by the specific sub-protocol. You must enter the sub-protocol in lower-case letters. Do not enter a port number.	• icmp/source-host-isolated • icmp/time-exceeded

8. Click **Apply**.
    - The newly created service group will appear at the bottom of the table.

⚠ For a complete list of supported services and sub-protocol, see Review supported services and sub-protocols.

Step 3: Create a Firewall Rule

1. In the Armor Management Portal (AMP), on the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top menu, click the corresponding data center.
4. Click **Actions**, and then click **New Rule**.
    - If you do not see **Actions**, then click **Create a Firewall Rule**.
5. In **Name**, enter a descriptive name.
6. In **Action**, select **Allow** to allow specified traffic to access your virtual machine or **Block** to block specified traffic.
7. Under **Service**, enter and select the name of the desired Service Group.
    - To learn how to create a Service Group, see Create a service group.
8. Under **Source**, enter and select the name of the desired IP Group.
    - To learn how to create an IP Group, see Create an IP group.
9. Under **Destinations**, in the field, enter and select the name of the desired IP Group.
10. Click **Save Rule**.

⚠ After you create a rule, Armor recommends that you place the rule in the correct order.

Reorder a rule:

1. Under Rule, in the numbered fields, enter a number to move the rule to a different position.
    - If you have more than 25 rules, the additional rules will be placed in a secondary section within the **Firewall**screen. To reorder and move these additional rules into a higher position, enter a number under the **Order**column, and then press **Enter** on your keyboard.
2. In the top menu that appears, click **Save**.

⚠ If you are not familiar with ordering rules, contact Armor Support to help you properly order your firewall rules. It is extremely important to order rules in order to receive desired traffic.

To learn how to send a support ticket, see Support Tickets.

Disable a rule:

1. Locate and hover over the desired rule.
2. Click the vertical ellipses.
3. Click **Disable Rule**.
4. Click **Disable Rule** again.
5. In the top menu that appears, click **Save**.

You can use Armor's StatusHub page to review the status of Armor's infrastructure, as well as other Armor services, such as the Armor Management Portal (AMP).

Additionally, you can use StatusHub to receive notifications and updates regarding infrastructure outages.

1. Access Armor's StatusHub page.
2. In the top menu, click **Subscribe**.
3. Select your desired notification method (**Email**, **SMS**, **Slack**, or **Webhook**), and then enter the corresponding information, such as your email address for the **Email** tab.
4. Select a notification type. There are two options.
    a. To receive information about every Armor service, click **All services**. This option will send you information about:
        i. All data centers
        ii. Armor API

iii. Gen 4 portal (amp.armor.com)

b. To receive information about specific Armor services, click **Selected Services**.
   i. Next to **Choose services**, click **Select**.
   ii. Click the desired data center, and then click **Select** to receive information for every infrastructure component for that data center.

5. During an unexpected outage (or incident), you may receive multiple updates regarding the status of an outage.
   - To receive multiple updates during an outage, select **OFF** for **Do not notify on intermediate incident updates**.
   - To simply receive one notification regarding the beginning of an outage, and then one notification regarding the completion of an outage, select **ON** for **Do not notify on intermediate incident updates**.
6. Click **Subscribe**.

Armor recommends that you configure your account to receive notifications for Account, Billing, and Technical events.

> ⚠ These notification preferences do not relate to support tickets.
>
> To update your notification preferences for support tickets, see Support Tickets.

Account	You will receive a notification when: • A password expires in 14 days. • A password expires in 7 days. • A password expires in 24 hours. • A password has expired.
Billing	You will receive a notification when: • An invoice has posted. • An invoice is past due (2, 10, 15, 25, and 30 days). • A payment method will soon expire (1, 15, and 30 days). ⚠ You can configure a user to become the primary billing contact for an account. This user will receive billing notifications. Additionally, this user will be listed in the **Bill to** field in an invoice. 1. In the Armor Management Portal (AMP), in the left-side navigation, click **Account**. 2. Click **Users**. 3. Locate and hover over the desired user. 4. Click the vertical ellipses. 5. Select **Set as Primary Billing Contact**. 6. Click **OK**.
Technical	You will receive a notification when: • A virtual machine will be deleted or downgraded. • CPU, disk, and memory utilization is at more than 90% for 5 minutes. • Ping, SSH (Linux), or RDP (Windows) fails for 5 minutes.

> ⚠ You can only change the notification preferences for your own account. You cannot change the notification preferences for other user accounts.

1. In the Armor Management Portal (AMP), in the top, right corner, click the vertical ellipses.
2. Click **Settings**.
3. Click **Notification Preferences**.
4. Use the slider to make your desired changes.
   - Select **Alert** to receive notifications in the top bar in the Armor Management Portal (AMP).
   - Select **Email** to receive notifications through email.
   - You can select both notification options.
5. Click **Update Notification Preference** to save your changes.

Was this helpful?

Your Rating: Results: 4 rates