

User Accounts

Armor Knowledge Base

Topics Discussed

- [Configure Multi-Factor Authentication \(MFA\) for your account](#)
- [Create and invite a user account](#)
- [Enable or disable a user account](#)
- [Accept and complete a user invitation](#)
- [Remove a newly created/invited user from your account](#)
- [Switch to another user account](#)
- [Change or reset your password](#)
- [Roles and Permissions](#)
- [Configure notification preferences](#)

Configure Multi-Factor Authentication (MFA) for your account

Each time you log into the Armor Management Portal (AMP), you must connect via a multi-factor authentication (MFA) method. There are two MFA methods:

- **Phone call**
 - Every time you log into AMP, you will receive a phone call. Answer the call, and follow the instructions to access AMP.
- **Phone application (Microsoft Authenticator)**
 - Every time you log into AMP, you will receive a message on your phone from the application. Open the application, and then click **Verify** to access AMP.

Configure MFA as a phone call

After you have configured your AMP account to use this method, every time you log into AMP, you will receive a phone call. Answer the call, and follow the instructions to access AMP.

1. In the Armor Management Portal (AMP), in the top, right corner, click the vertical ellipses.
2. In the drop-down menu, select **Settings**.
3. Click **Security + Authentication**.
4. For **MFA Settings**, click **Phone Call**.
5. In **Country**, select your country's abbreviation and country code.
6. In **Phone Number**, enter your phone number.
 - You can include spaces and special characters.
7. (Optional) In **Extension**, enter your phone number's extension.
 - You can only include numbers.
 - Do not enter "x" or "ext."
8. Click **validate your new phone number**. This process may take a few minutes.
9. When your phone rings, answer the phone and follow the instructions.



Every time you log into AMP, you will receive a phone call. Answer the call, and follow the instructions to access AMP.

10. Click **Save Changes**.
 - (Optional) To deactivate the phone call method and use the Microsoft Authenticator method, see [Configure MFA with Microsoft Authenticator application](#).

Configure MFA as a phone application (Microsoft Authenticator)



This application is available to iPhone users and Android users.

You cannot use the Multi-Factor Authentication (MFA) application from Microsoft on your first login into the Armor Management Portal (AMP). You must first access AMP via the phone call method. After you log into AMP, you can then configure your account to use the application from Microsoft.

After you have configured your AMP account to use this application, every time you log into AMP, you will receive a message on your phone device from the application. Open the application, and then click **Verify** to access AMP.

1. In the Armor Management Portal (AMP), in the top, right corner, click the vertical ellipses.
2. In the drop-down menu, select **Settings**.
3. Click **Security + Authentication**.
4. For **MFA Settings**, click **Microsoft Authenticator**.

5. Click **Configure App**.
6. In your phone device, download the application called **Microsoft Authenticator**.
7. Open the application.
8. (Optional) For some users, you must allow the application to send you notifications.
9. In your phone device, click **Add account**.
10. Select an account type.
11. (Optional) For some users, you must allow the application to access your phone's camera.
12. When the camera is activated, scan the QR code that appears in AMP.
13. When a new account has been created in the application, click **I have scanned the QR** in AMP.
14. Click **Verify & Apply MFA Changes**. This step may take a few minutes to complete.



Every time you log into AMP, you will receive a message on your phone from the application. Open the application, and then select **Verify** or **Approve** to access AMP. The application does not need to be opened for you to receive the authentication request.

- (Optional) To deactivate the Microsoft Authenticator and use the phone method, see [Configure MFA as a phone call](#).

Troubleshoot MFA for a new phone device or phone number

Every time you log into the Armor Management Portal (AMP), you must connect via a multi-factor authentication (MFA) method that is specific to your phone device or phone number. As a result, if you change your phone device or phone number, you may need to perform additional steps in order to maintain access to your AMP account.

Review the following scenarios to learn how to maintain access to your AMP account:

You can use these instructions if you:

- Will soon switch phone devices
- Have both phone devices available

1. In the Armor Management Portal (AMP), in the top, right corner, click the vertical ellipses.
2. In the drop-down menu, select **Settings**.
3. Click **Security + Authentication**.
4. For **MFA Settings**, click **Phone Call**.
5. In **Country**, select your country's abbreviation and country code.
6. In **Phone Number**, enter the phone number of the new phone.
 - You can include spaces and special characters.
7. (Optional) In **Extension**, enter your phone number's extension.
 - You can only include numbers.
 - Do not enter "x" or "ext."
8. Click **validate your new phone number**. This process may take a few minutes.
9. When your phone rings, answer the phone and follow the instructions.



Every time you log into AMP, you will receive a phone call. Answer the call, and follow the instructions to access AMP.

10. Click **Save Changes**.
11. Turn off your old phone device, and then turn on your new phone device.
12. Login to your AMP account.
 - You will receive a phone call on your new phone device. When your phone rings, answer the phone and follow the instructions.
13. In AMP, in the top, right corner, click the vertical ellipses.
14. In the drop-down menu, select **Settings**.
15. Click **Security + Authentication**.
16. For **MFA Settings**, click **Microsoft Authenticator**.
17. Click **Configure App**.
18. In your new phone device, download the application called **Microsoft Authenticator**.
19. Open the application.
20. (Optional) For some users, you must allow the application to send you notifications.
21. In your phone device, click **Add account**.
22. Select an account type.
23. (Optional) For some users, you must allow the application to access your phone's camera.
24. When the camera is activated, scan the QR code in AMP.
25. When a new account has been created in the application, click **I have scanned the QR** in AMP.
26. Click **Verify & Apply MFA Changes**. This step may take a few minutes to complete.

You can use these instructions if you:

- Used the phone call method to access AMP
- Already switched to a different phone number

1. Contact Armor Support to update your phone number.
 - For the United States office, call + 1 877 262 3473. For the United Kingdom office, call +44 800 500 3167.

You can use these instructions if you:

- Used the phone application (Microsoft Authenticator) to access AMP
- Already switched to a different phone device

1. Contact Armor Support to update your phone number.
 - For the United States office, call + 1 877 262 3473. For the United Kingdom office, call +44 800 500 3167.
 - Internally, Armor Support will change your MFA preference to the phone call method. Afterwards, once you access AMP via the phone call method, you can update your MFA preference.



After you access AMP, you can update your MFA preferences and use the phone application (Microsoft Authenticator) method. To learn more, see [Configure MFA via Microsoft Authenticator application](#).

Create and invite a user account

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Account**.
2. Click **Users**.
3. Click the plus (+) icon.
4. Complete the **First Name**, **Last Name**, and **Email Address** fields.
 - The email address you enter will be the username.
5. Select a role for this user.
 - You must assign a role to the user.
 - You can assign multiple roles to the user.
 - You can assign a default role (Admin, Technical, Billing).
 - **Admin** contains every permission in AMP.
 - **Technical** contains mostly write-only permissions.
 - **Billing** contains mostly read-only permissions
 - To learn about Roles and Permissions, see [Roles and Permissions](#).
6. Click **Create User**. An email will be sent to the user. After 96 hours, the sign-up link in the email will expire.
 - If the link expires, you can resend the user invitation. In the **Users** screen, hover over the desired user, click the vertical ellipses, and then select **Resend Invitation**.
 - If you want to remove this newly created / invited user from your account, see [Remove a newly created / invited user from your account](#).

Accept and complete a user invitation

Step 1: Open the Account Signup email

1. In the email from Armor, click the link.
 - You will be redirected to enter your account security information, including payment information.
 - If you already coordinated your payment process with Armor, then you will not see the payment screen.

Step 2: Complete your 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**.



If you already coordinated with Armor to pay with a check, then you will be redirected to Armor Management Portal (AMP) login screen..

Step 3: Complete your payment information

1. In **Currency**, select your currency.

2. (Optional) If your business is tax exempt, select **I'm tax exempt**.
 - In **Tax Exempt ID**, enter a valid tax exempt ID.
3. For **Payment Method**, mark the desired payment (credit card or bank account).

Option 1: Credit card



Cardholder Name, Address, City, State, and Postal Code will be pre-populated with the name and contact information for the **Primary Contact** on the account.

1. In **Card Number**, enter the credit card number.
2. In **Expiration Date**, select the appropriate month and year.
3. In **CVV**, enter the verification number for the credit card
4. In **Country**, select the corresponding country.
5. Click **Submit**.



You will be redirected to Armor Management Portal (AMP) login screen.

Option 2: ACH Bank Debit

1. In **ABA / Routing Number**, enter the corresponding banking number.
2. In **Bank Account Number**, enter the account number.
3. Select the appropriate **Account Type**.
4. In **Bank Name**, enter the name of the banking institution.
5. In **Account Holder Name**, enter the name of the account holder.
6. Click **Submit**.



You will be redirected to Armor Management Portal (AMP) login screen.

Remove a newly created / invited user from your account

You can remove a user account that is in the **Invited** status or **Enabled** status.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Account**.
2. Click **Users**.
3. Locate the newly created user.
4. Hover over the user, and then click the vertical ellipses.
5. Select **Remove User from Account**.
6. Click **OK**.

Enable or disable a user account



A user cannot disable or enable their own user account.



When you disable a user, you also disable the ability to edit their roles. You cannot add or remove a disabled user's roles.

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. Click **Enable** or **Disable**.
6. Click **OK**.

 After you disable a user, you can then remove a user from your account.

 A user cannot remove their own user account.

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 **Remove User from Account**.
6. Click **OK**.

Switch to another user account

If you have multiple Armor Management Portal (AMP) accounts, you can simply switch to another user account. You do not have to logout and login again to access your other accounts.

You can switch accounts while inside a specific page without being redirected to the home page. This function exists when you switch to another account that contains the same, corresponding page.

1. In the Armor Management Portal (AMP), in the top, right corner, click the vertical ellipses.
2. In the menu that appears, select the desired account. The screen will automatically refresh and load the selected account.

Update basic profile information

1. In the Armor Management Portal (AMP), in the top, right corner, click the vertical ellipses.
2. Click **Settings**.
3. Make your desired changes.
4. Click **Update User**.

Change your password

To create a secure login for your account, Armor recommends that you use a passphrase, and not a password.

A passphrase is a combination of seemingly unrelated words; a password tends to be a single word, followed by numbers and special characters. To increase the strength of your passphrase, you can add numbers, special characters, and a mix of upper-case and lower-case letters.

For example, you can enhance the passphrase **armoravocadosummer** to **armor@vocado\$uMM3er**.

 When you create and change your password in AMP, consider the following statements:

- You can only change your password once every 24 hours.
- Passwords expire after 60 days.
- You cannot use any of your previous 24 passwords.
- After 6 failed login attempts, you will be locked out of your account for an hour.
 - You will be notified via email.
 - An account administrator on your account or Armor support can unlock your account.
- After 15 minutes of inactivity, you will be logged out of the Armor Management Portal (AMP).
- You will receive an email from Armor to confirm that you have changed your password. If you wrongly receive this email, you must contact Armor immediately.

1. In the Armor Management Portal (AMP), in the top, right corner, click the vertical ellipses.
2. Click **Settings**.
3. Click **Security + Authentication**.
4. In **Old Password**, enter your current password.
5. In **Password** and **Password (Confirm)**, enter a new password.
 - Your password must contain the following requirements:
 - At least 12 characters long
 - An upper-case letter
 - A lower-case letter
 - A number
 - 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.
6. Click **Update Password**.

Reset a forgotten password

 You can only change your password once every 24 hours.

 You can reset your password via email or via SMS.

Reset a password via email

1. In the login page, click **Forgot Password**.
2. Enter the email address associated with your user account, and then click **Choose Recovery Method**.
3. Select **Email**.
 - An email will be sent to the email address associated with your user account.
4. Click the link in the email.
5. Enter a new password; re-enter the password to confirm, and then click **Set New Password**.
 - You will receive an error message if:
 - Your passwords do not match.
 - Your password does not meet the password requirements.
 - Your password was changed less than 24 hours ago.
 - Your password was recently used. (You cannot use any of your previous 24 passwords.)
6. After you reset your password, you will receive a phone call in order to authenticate. Answer the phone call, and then enter the pound (#) sign. Your screen will refresh to the landing page for the Armor Management Portal (AMP).

Reset a password via SMS

1. In the login page, click **Forgot Password**.
2. Enter the email address associated with your user account, and then click **Choose Recovery Method**.
3. Select **Text Message**.
 - A text message will be sent to the phone number listed in your user account.
4. Enter the verification code from the text message.
5. Enter a new password; re-enter the password to confirm, and then click **Set New Password**.
 - You will receive an error message if:
 - Your passwords do not match.
 - Your password does not meet the password requirements.
 - Your password was changed less than 24 hours ago.
 - Your password was already used. (You cannot use any of your previous 24 passwords.)
6. After you reset your password, you will receive a phone call in order to authenticate. Answer the phone call, and then enter the pound (#) sign. Your screen will refresh to the landing page for the Armor Management Portal (AMP).

Roles and Permissions

Create a role and add permissions

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Account**.
2. Click **Roles + Permissions**.
3. Click the plus (+) icon.
4. In the top, right corner of the screen, hover over the gear icon.
5. Click the blue pencil (**Rename**) icon.
6. In the window that appears, enter a descriptive name, and then click **Rename Role**.
7. In the top menu, click **Members**.
8. In the field, enter and select the user (or users) to assign to the role.
9. In the top menu, click **Permissions**.
10. Mark the permissions to add to your role.
11. At the bottom of the screen, click **Save Role**.

Assign a role to an existing user account

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Account**.
2. Click **Roles + Permissions**.
3. Locate and select the desired role.

4. In the top menu, click **Members**.
5. In the field, enter and select the desired user.
 - The change will be automatically saved.
 - The user will have immediate access to the permissions within the role.
6. (Optional) To remove a user, hover over the desired user, click the trash icon, and then click **Remove user access**.

Configure notification preferences

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	<p>You will receive a notification when:</p> <ul style="list-style-type: none"> • A password expires in 14 days. • A password expires in 7 days. • A password expires in 24 hours. • A password has expired.
Billing	<p>You will receive a notification when:</p> <ul style="list-style-type: none"> • 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). <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> 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.</p> <ol style="list-style-type: none"> 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. </div>
Technical	<p>You will receive a notification when:</p> <ul style="list-style-type: none"> • 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.

The above notifications preference types are not available unless the user is assigned one of the following permissions:

Account	Billing	Technical
<ul style="list-style-type: none"> • Read Identity • Update Personal Identity • Write Identity 	<ul style="list-style-type: none"> • Update Payment Information • View Invoices • Read Product Catalog • View Subscriptions • Write Subscriptions 	<ul style="list-style-type: none"> • Read Workload(s) • Write Workload • Read Virtual Machine(s) • Write Virtual Machine



Was this helpful? *

Your Rating:

Results: 14 rates