

Roles and permissions (Armor Anywhere)

[Home](#) > [AMP Account User Guides](#) > [Roles and permissions \(Armor Anywhere\)](#)

This topic only applies to **Armor Anywhere** users.

Overview

This topic only applies to **Armor Anywhere** users. If you are an **Armor Complete** user, see [Roles and Permissions \(Armor Complete\)](#).

In the Armor Management Portal (AMP), **roles** are similar to job titles that you must create and assign to your users. When you create a new role, you can populate that role with specific **permissions**. These permissions determine the type of access a user has in AMP. For example, you can create an **Accounting** role, and then you can add specific permissions to only give the user access to accounting-related features in AMP, such as the permission to view invoices.

When you create a new user, you must assign that user a role.

Create and assign a new role

Step 1: Create a role and add permissions

To see a list of available permissions, see [Review available 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**.

Step 2: 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.

Update a permission for a role

You cannot edit the permissions within a default role.

Remember, when you update the permissions for a role, the users assigned to that role will automatically be able to use the newly added permissions.

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. Mark (or unmark) the desired permissions.
5. Click **Save Role** in the bottom of the screen.

Remove a role for a newly created or existing user

After you create a user account with an assigned role, the new user will receive an email to complete the account creation process. During this time, the account administrator has limited access to that user account; however, the account administrator can still update roles and permissions for the newly created user.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Account**.
2. Click **Roles + Permissions**.
3. In the search field, enter the name of the user, and click the magnifying glass icon.
 - The table will display the roles assigned to the user.
4. Click the desired role.
5. In the top menu, click **Members**.
6. In the table, place the cursor over the user, and then click the trash icon.
7. Click **Remove Access**.

Delete a role

You do not need to remove the permissions from a role in order to delete a role.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Account**.
2. Click **Roles + Permissions**.
3. Locate and hover over the desired role.
4. Click the vertical ellipses.
5. Click **Delete**.
6. Click **Delete Role**.

Review permissions for popular AMP screens

Review the following tables to understand the permissions needed to interact with popular screens in AMP.

To view every permission available in AMP, see [Review all permissions](#).

In the **Roles and Permissions** screen, you may see permissions that only apply to **Armor Complete** users. Your roles will not malfunction if you happen to add an **Armor Complete** permission to your role.

Permissions for virtual machines

Screen / Feature	Actions	Permissions	Additional information
Virtual Machines	<ul style="list-style-type: none"> • Create a virtual machine • Update a virtual machine • Delete a virtual machine • View the core license to download and install the agent 	<ul style="list-style-type: none"> • Write Virtual Machine • View Core License 	<p>To learn more about the Virtual Machines screen, see Virtual Machines (Armor Anywhere).</p>

Permissions for Cloud Connection

Screen / Feature	Actions	Permissions	Additional information
Cloud Connections	<ul style="list-style-type: none"> • Collect and store logs with the Log Depot add-on product <ul style="list-style-type: none"> • To specifically collect CloudTrail logs, see Collect and view CloudTrail logs in AMP. • View the security status of your virtual machine in the Virtual Machines screen 	<ul style="list-style-type: none"> • Read Cloud Connections • Write Cloud Connections 	<p>To learn more about Cloud Connections, see Cloud Connections.</p>

Permissions for support tickets

Screen / Feature	Actions	Permissions	Additional information
Tickets + Notifications	<ul style="list-style-type: none"> • Create a support ticket • View a support ticket • Add a recipient to an existing support ticket • Chat with Armor 	<ul style="list-style-type: none"> • Read Ticket(s) • Write Ticket(s) 	<p>In addition to these permissions, in order to view a ticket, you must be listed as a recipient. For example, if a user in your account sends a support ticket, and you are not listed as a recipient, then you will not be able to see this ticket.</p> <p>To learn more about the Tickets + Notifications screen, see Support Tickets.</p>

Permissions for Log & Data Management

Screen / Feature	Actions	Permissions	Additional information
Log & Data Management	<ul style="list-style-type: none"> • View collected logs in the Search section • View the status of the logging subagent in the Sources section 	<ul style="list-style-type: none"> • Write LogManagement • Read LogManagement 	<p>To learn more about Log Management, see Log Management (Armor Anywhere).</p>

Permissions for the Health Dashboards

Screen / Feature	Actions	Permissions	Additional information
<ul style="list-style-type: none">Health Overview (landing screen)<ul style="list-style-type: none">ProtectionDetectionResponseSecurity Incidents	<ul style="list-style-type: none">View the data that populates the security dashboards	<ul style="list-style-type: none">Read Dashboard Statistics	<p>To learn more about the dashboards, see Health Overview Dashboard (Armor Anywhere).</p>

Permissions for Security screens

Screen / Feature	Actions	Permissions	Additional information
<ul style="list-style-type: none">Security screens<ul style="list-style-type: none">Malware ProtectionFile Integrity Monitoring (FIM)Patching	<ul style="list-style-type: none">View the data that populates the security-focused screens	<ul style="list-style-type: none">Read AVAMRead FIMRead OS Packages	<p>To learn more, see:</p> <ul style="list-style-type: none">Malware Protection (Armor Anywhere)File Integrity Monitoring (FIM) (Armor Anywhere)Patching (Armor Anywhere)