Introduction to Roles and Permissions

Armor Knowledge Base

Topics Discussed

Review the following **Frequently Asked Questions** to better understand how roles and permissions affect your access into the Armor Management Portal (AMP).

What are Permissions?

In the Armor Management Portal (AMP), every screen (and functionality within the screen) is protected by various permissions. In order to access and use a specific screen in AMP, you must have the appropriate permissions added to your account.

For example, to create and manage a virtual machine within the **Virtual Machines** screen in AMP, you must have access to the following permissions in your account:

- Read Workload(s)
- Write Workload
- Read Virtual Machine Stats
- Read Virtual Machine(s)
- Write Virtual Machine
- Scale Virtual Machine
- Read Location(s)
- Read Virtual Data Centers
- Read Tasks
- Write Tasks
- Read Storage
- Read Network L2L
- Write Network L2L
- Read SSL VPN Devices and Users
- Write SSL VPN Devices and User

What are Roles?

A role is similar to a job title that you must assign to your users. Each role is made up of several permissions, designed to control the access your users have in the Armor Management Portal (AMP).

You cannot assign a permission directly to a user; you must add a permission to a role, and then assign that role to a user.

Every user in AMP, including account administrators, must have a role assigned to their account. Users can have multiple roles assigned to their account.

Frequently Asked Questions (FAQ)

If I am an account administrator, who creates my role?

Armor will automatically assign the **Admin** role to every account administrator. By default, the **Admin** role will contain every permission available in AMP.

If I am not the account administrator, who creates my role?

The account administrator will use the Armor Management Portal (AMP) to create new users. During this process, the account administrator will assign a role to the new user. The account administrator can select a default role (with permissions already included) or create a new role.

The account administrator cannot successfully create a new user without assigning a role to the new user.

To learn how to assign a role, see Assign a role to a user.

What roles should I create?

You can create any type of role based on the needs of your organization. Consider your users and the type of permission you want these users to have in the Armor Management Portal (AMP).

For example, if you need to create a user who will only focus on billing information in AMP, such as invoices and payment methods, you can create an **Acc ounting** role, and then populate that role with permissions that only relate to the **Invoices** screen and the **Payment Methods** screen.

Other popular roles to consider are:

- Security
  - You can create a Security role to allow users to review security-related data, such as patching or malware information.
- Technical
  - You can create a Technical role to allow users to create and manage virtual machines, firewall rules, IP addresses, etc.

> ⚠ If your AMP account contains few users, then consider assigning the Admin role to your users. The Admin contains every permissions in AMP, which can make user management easier for you.

Are there any default roles?

Yes. Armor creates three default roles that are already populated with permissions:

- Admin
- Technical
- Billing

> ⚠ In AMP, you can easily identify a default role by the orange Armor badge that displays next to the role name.

For your convenience, when you create a new user, you can assign a default role to that user; however, you cannot edit the permissions within these default roles.

To learn more about these default roles, see Review default roles and corresponding permissions.

What happens when Armor creates a new permission? Is that permission automatically added to a role?

Armor offers the following three default roles that are already populated with permissions:

- Admin
- Technical
- Billing

When a new permission is added to AMP, the permission is automatically added to the appropriate default role. For instance, if Armor introduces a new permission related to virtual machines, then that permission will be automatically added to the **Admin** and **Technical** roles.

However, for any role that you create, you must add the new permission to your role.

Can I update a role by removing or adding new permissions?

Yes. In the Armor Management Portal (AMP), you can update a role by removing or adding permissions. When you save your changes, the changes will take place immediately.

> ⚠ You cannot update a default role created by Armor.

How do I create a role and populate that role with permissions?

To learn how to create a new role with permissions, see Create and assign a new role.

Why did Armor protect every screen and feature with a permission?

As a security-focused company, Armor wants to ensure that only the appropriate users in your organization can access the sensitive data displayed in the Armor Management Portal (AMP). As a result, Armor has designed AMP to allow account administrators to decide which users can access specific screens in AMP.

Is there documentation to explain how to use the Roles and Permissions screen in AMP?

Yes. For more information, see Roles and Permissions.

Was this helpful?

Your Rating: ☆☆☆☆☆ Results: ★★★★★ 4 rates