Roles and Permissions

Armor Knowledge Base

Topics Discussed

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.

There are two ways to assign a user to a role:

1. Assign a default role with permissions already enabled in AMP.
   - To learn more, see Assign a default role.
2. Create a new role, populate that role with your preferred permissions, and then assign that role to a user.
   - To learn more, see Create and assign a new role.

To review Frequently Asked Questions (FAQs) regarding roles and permissions in AMP, see Introduction to Roles and Permissions.

Assign a Default Role

Step 1: Review default roles and corresponding permissions

If your AMP account was created before May 2017, then by default, you will only see the **Admin** role. This role contains every permission available.

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

You cannot edit the permissions within the default roles.

The default **Admin** role contains every permission available.

This role is automatically updated with new permissions after an AMP release.

This role is automatically assigned to a new administrator account.

At a high-level, the default **Billing** role contains mostly read-only permissions.

This role is not automatically updated with new permissions after an AMP release.

Review the following table to better understand the specific permissions associated with the default **Billing** role.

AMP Screen	Permission	Description

Security Dashboard (landing page)	Read Dashboard Statistics	This permission allows you to view the widgets (and corresponding data) that populate the security dashboard. These widgets display a high-level status of your virtual machines, agents, and open security incidents.
Malware Protection	Read AVAM	This permission allows you to view antivirus and anti-malware (malware protection) details for each virtual machine.
FIM	Read FIM	This permission allows you to view file integrity details for each virtual machine.
Patching	Read OS Packages	This permission allows you to view details OS patching details for each virtual machine.
Intrusion Detection	Read IDS	This permission allows you to view intrusion detection data.
Log & Data Management	Read LogManagement	This permission allows you to view high-level information for log collection for each virtual machine, such as: • Date logs were last received • Average size of collected logs • Log Status
Log & Data Management	Read LogSearch	This permission allows you to view details for log collection, such as the specific log message, for each virtual machine.
Firewall	Read Firewall	This permission allows you to view details for firewall rules for each virtual machine.
Marketplace	Read Product Catalog	This permission allows you to view available add-on products. You must have this permission enabled in your account in order to view purchased services and also to order new services in AMP.
Marketplace (and My Products)	View Subscriptions	This permission allows you to view subscription-based add-on products in the My Products screen of the User Details screen.
Workloads	Read Workload (s)	This permission allows you to view high-level data for workloads, such as • the associated data center • the number of tiers within the workload • the number of virtual machines within the workload
Virtual Machines	Write Orders	This permission allows you to provision a new virtual machine.
Virtual Machines	Read Virtual Machine Stats	This permission allows you to view usage data for a virtual data. This data is displayed in a line graph.
Virtual Machines	Read Virtual Machine(s)	This permission allows you to view data for a virtual machine, such as • Operating system • Size • Corresponding workload • Status
Virtual Machines	Read Location (s)	This permission allows you to view a list of available Armor data centers when you manage your virtual machines.
Virtual Machines	Read Virtual Data Centers	This permission allows you to view the list of virtual environments in your account.
Virtual Machines	Read Server Replication	This permission allows you to view high-level data for the server replication (disaster recovery) add-on product. Specifically, this permission allows you to view: • The status of the add-on product (configuring, enabled, disabled) • The location of the primary data center • The location of the failover data center • The status of the replication
Virtual Machines	Read Tasks	This permission allows you to view pending tasks, such as a scheduled delete or downsize of a virtual machine.
Virtual Machines	Read Storage	This permission allows you to view disk and storage information for a virtual machine.
IP Addresses	Read Network IP	This permission allows you to view data for unassigned and assigned public and private IP addresses

IP Addresses	Read Network NAT	This permission allows you to view DNAT assignments.
L2L VPN	Read Network L2L	This permission allows you to view high-level data for your L2L network tunnels.
SSL/VPN	Read SSL VPN Devices and Users	This permission allows you to view the status of your users' SSL VPN client.
Compliance	Read Compliance	This permission allows you to view information for the vulnerability scanning add-on product information. Specifically, you will see the status of the add-on product.
Tickets	Read Ticket(s)	This permission allows you to view support tickets listed in the **View Archived Tickets** section.
Overview (Account screen)	Read Identity	This permission allows you to view the account-level information, such as • Account overview • Armor contacts • User profiles • Roles and permissions
User Detail	Update Personal Identity	This permission allows you to update your personal account information, such as your: • Password • Challenge Phrase • Challenge Response
User Detail	Read Notification(s)	This permission allows you to view the notification preferences for your users, such as a user's preference to receive an email regarding technical updates.
Invoices	View Invoices	This permission allows you to view current and previous invoices.
Payment Methods	Read Payment Information	This permission allows you to view current payment information, such as the primary payment method.
Payment Methods	Write / Update Payment Information	This permission allows you to update the payment information, such as adding a new credit card or assigning a new primary payment method
Not applicable	Read Entity Metadata	This permission allows you to view optional notes and tags that have been added to various AMP resources, such as a note added to a virtual machine.
Not applicable	Write Entity Metadata	This permission allows you to add, update, and delete optional notes and tags to various AMP resource, such as adding a note to a virtual machine.
Not applicable	Global Search	This permission allows you to use the global search function throughout AMP.

At a high-level, the default **Technical** role contains read-only and write-only permissions, with a focus on security and infrastructure resources in AMP.

⚠ This role is not automatically updated with new permissions after an AMP release.

Review the following table to better understand the specific permissions associated with the default **Technical** role.

AMP Screen	Permission	Description
Security Dashboard (landing page)	Read Dashboard Statistics	This permission allows you to view the widgets (and corresponding data) that populate the security dashboard. These widgets display a high-level status of your virtual machines, agents, and open security incidents.
Malware Protection	Read AVAM	This permission allows you to view antivirus and anti-malware (malware protection) details for each virtual machine.
FIM	Read FIM	This permission allows you to view file integrity details for each virtual machine.
Patching	Read OS Packages	This permission allows you to view details OS patching details for each virtual machine.
Intrusion Detection	Read IDS	This permission allows you to view intrusion detection data.

Log & Data Management	Read LogManagement	This permission allows you to view high-level information for log collection for each virtual machine, such as: • Date logs were last received • Average size of collected logs • Log Status
Log Management	Read LogSearch	This permission allows you to view details for log collection, such as the specific log message, for each virtual machine.
Log Management	Write LogManagement	This permission allows you to update the log management service, specifically the permission to upgrade the log retention plan.
Firewall	Read Firewall	This permission allows you to view details for firewall rules for each virtual machine.
Firewall	Write Firewall	This permission allows you to add, update, or delete firewall rules.
Marketplace	Read Product Catalog	This permission allows you to view available add-on products. You must have this permission enabled in your account in order to view purchased services and also to order new services in AMP.
Marketplace (and My Products)	View Subscriptions	This permission allows you to view subscription-based add-on products in the My Products screen of the User Details screen.
Marketplace (and My Products)	Write Subscriptions	This permission allows you to view the Armor Marketplace, as well as add and cancel subscription-based add-on products. Specifically, you can add the subscription in the Armor Marketplace, and then cancel the subscription in the My Products screen of the User Details screen.
Workloads	Read Workload (s)	This permission allows you to view high-level data for workloads, such as • the associated data center • the number of tiers within the workload • the number of virtual machines within the workload
Workloads	Write Workload	This permission allows you to create, update, and remove workloads and tiers.
Virtual Machines / VM Details	Write Orders	This permission allows you to provision a new virtual machine.
Virtual Machines / VM Details	Read Virtual Machine Stats	This permission allows you to view usage data for a virtual data. This data is displayed in a line graph.
Virtual Machines / VM Details	Read Virtual Machine(s)	This permission allows you to view data for a virtual machine, such as • Operating system • Size • Corresponding workload • Status
Virtual Machines / VM Details	Scale Virtual Machine	This permission allows you upgrade or downgrade (resize) the size of a virtual machine.
Virtual Machines / VM Details	Write Virtual Machine	This permission allows you to create, update, and remove virtual machines.
Virtual Machines / VM Details	Read Location (s)	This permission allows you to view a list of available Armor data centers when you manage your virtual machines.
Virtual Machines / VM Detail	Read Virtual Data Centers	This permission allows you to view the list of virtual environments in your account.

Virtual Machines	Read Server Replication	This permission allows you to view high-level data for the server replication (disaster recovery) add-on product. Specifically, this permission allows you to view: • The status of the add-on product (configuring, enabled, disabled) • The location of the primary data center • The location of the failover data center • The status of the replication
Virtual Machines	Write Server Replication	This permission allows you to order and cancel the server replication add-on product.
Virtual Machines	Read Tasks	This permission allows you to view pending tasks, such as a scheduled delete or downsize of a virtual machine.
Virtual Machines	Write Tasks	This permission allows you to schedule a delete or downsize of a virtual machine.
Virtual Machines	Read Storage	This permission allows you to view disk and storage information for a virtual machine.
IP Addresses	Read Network IP	This permission allows you to view data for unassigned and assigned public and private IP addresses
IP Addresses	Write Network IP	This permission allows you to update an IP address, such as: • Assign an IP addresses • Unassign an IP addresses • Delete IP address • Request a new public IP address
IP Addresses	Read Network NAT	This permission allows you to view DNAT assignments.
IP Addresses	Write Network NAT	This permission allows you to add and remove DNAT assignments.
L2L VPN	Read Network L2L	This permission allows you to view high-level data for your L2L network tunnels.
L2L VPN	Write Network L2L	This permission allows you to add, update, and remove L2L tunnels.
SSL/VPN	Read SSL VPN Devices and Users	This permission allows you to view the status of your users' SSL VPN client.
SSL/VPN	Write SSL VPN Devices and User	This permission allows you to enable your users the ability to download and install the SSL VPN client.
Compliance	Read Compliance	This permission allows you to view information for the vulnerability scanning add-on product information. Specifically, you will see the status of the add-on product.
Compliance	Write Compliance	This permission allows you to upgrade, downgrade, or delete the vulnerability scanning add-on product.
Tickets	Read Ticket(s)	This permission allows you to view support tickets listed in the **View Archived Tickets** section.
Overview (Account screen)	Read Identity	This permission allows you to view the account-level information, such as • Account overview • Armor contacts • User profiles • Roles and permissions
User Detail	Update Personal Identity	This permission allows you to update your personal account information, such as your: • Password • Challenge Phrase • Challenge Response
User Detail	Read Notification(s)	This permission allows you to view the notification preferences for your users, such as a user's preference to receive an email regarding technical updates.
Not applicable	Read Entity Metadata	This permission allows you to view optional notes and tags that have been added to various AMP resources, such as a note added to a virtual machine.
Not applicable	Write Entity Metadata	This permission allows you to add, update, and delete optional notes and tags to various AMP resource, such as adding a note to a virtual machine.

Not applicable	Global Search	This permission allows you to use the global search function throughout AMP.

Step 2: Assign a default role

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Account**.
2. Click **Roles + Permissions**.
3. Locate and select the desired default role (**Admin**, **Billing**, or **Technical**).
4. Click **Members**.
5. Under **Members**, enter and select the name of the user.

Create and assign a new role

Step 1: 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**.

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 crated 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**.

Additional Documentation

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** or **Armor Anywhere** users. Your roles will not malfunction if you happen to add a permission for a different product to your role.

Was this helpful?

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