Generation 4 Upgrade Information

⚠ Before you begin, to better understand the upgrade process, Armor recommends that you review the FAQs for Generation 4 Upgrade documentation.

⚠ This document only applies to **Armor Complete** account administrators who have been notified by Armor to perform two pre-upgrade tasks.

24 hours before your scheduled upgrade begins, you will receive an invitation from Armor to complete the account signup process to access the **Armor Management Portal (AMP)**.

Before the upgrade process begins, Armor recommends that you complete the two tasks below so that after the upgrade process is complete, you and your users can easily access AMP.

Step 1: Complete your account signup

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 beredirected 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.

Step 2: Review assigned roles

In the Armor Management Portal (AMP), **roles** are similar to job titles that you can create and assign to your users. You can populate these roles with specific **permissions** to restrict the type of access your users can have in AMP.

For example, if you have a user who simply needs accounting permissions in AMP, you can create an **Accounting** role, assign accounting-related permissions to the role, and then assign the **Accounting** role the specific user.

To prepare for the upgrade process, Armor has:

- Created three default roles (**Admin**, **Technical**, and **Billing**) with permissions
- Transferred your users into AMP
- Assigned one of the default roles to your users

Step 1: View default roles and permissions

Armor recommends that you review the assigned roles, along with their corresponding permissions.

Permissions

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

The **Admin** role is automatically assigned to a new administrator account.

To review every available permission, see Review available permissions.

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

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 permissions 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 permissions allows you to view antivirus and anti-malware (malware protection) details for each virtual machine.
FIM	Read FIM	This permissions allows you to view file integrity details for each virtual machine.
Patching	Read OS Packages	This permissions allows you to view details OS patching details for each virtual machine.
Log Management	Read LogManagement	This permissions 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.
Firewall	Read Firewall	This permissions 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 / 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	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 Details	Read Virtual Data Centers	This permission allows you to view the list of virtual environments in your account.
Virtual Machines / VM Details	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 / VM Details	Read Tasks	This permission allows you to view pending tasks, such as a scheduled delete or downsize of a virtual machine.
Virtual Machines / VM Details	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 + Notification	Read Ticket(s)	This permission allows you to view previous and current support tickets.

Tickets + Notification	Write Ticket(s)	This permission allows you to create and follow a support ticket.
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.

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 permissions 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 permissions allows you to view antivirus and anti-malware (malware protection) details for each virtual machine.
FIM	Read FIM	This permissions allows you to view file integrity details for each virtual machine.
Patching	Read OS Packages	This permissions allows you to view details OS patching details for each virtual machine.
Log Management	Read LogManagement	This permissions 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 permissions allows you to view details for firewall rules for each virtual machine.
Firewall	Write Firewall	This permissions 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 + Notification	Read Ticket(s)	This permission allows you to view previous and current support tickets.
Tickets + Notification	Write Ticket(s)	This permission allows you to create and follow a support ticket.
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.

(Optional) Step 2: Update assigned roles

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Account**.
2. Click **Roles + Permissions**.
3. Click **Admin**.
4. Click **Members**.
5. Review and confirm the list of assigned users.
6. (Optional) To remove a user from this role, in the table, hover over the desired user, click the trash icon, and then click **Remove Access**.
7. In the left-side navigation, click **Roles + Permissions**.

8. Click **Billing**.
9. Click **Members**.
10. Review and confirm the list of assigned users.
11. (Optional) To remove a user from this role, in the table, hover over the desired user, click the trash icon, and then click **Remove Access**.
12. In the left-side navigation, click **Roles + Permissions**.
13. Click **Technical**.
14. Click **Members**.
15. Review and confirm the list of assigned users.
16. (Optional) To remove a user from this role, in the table, hover over the desired user, click the trash icon, and then click **Remove Access**.

Was this helpful?

Your Rating: Results: 3 rates