


Complete the onboarding process and install the Armor Anywhere agent (Windows 2012 and 2016)

In This Document

Have a suggestion for the Armor Knowledge Base? Send a message to kb@armor.com.

 [Home](#) > [Installation](#) > [Complete the onboarding process and install the Armor Anywhere agent \(Windows 2012 and 2016\)](#)

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

For invited users:


Before your account was created, your account administrator decided the proper roles and permissions for your account.


Consult with your account administrator to understand what permissions you have and how you should configure your account.

You can use this document to complete the account signup process and review high-level action items to complete.


 This topic only applies to users who run:

- Windows 2012 Datacenter
- Windows 2012 R2 Standard
- Windows 2012 Standard
- Windows 2016 Full Desktop

 For Windows 2012 users, when you install the Armor Agent, the corresponding Trend Micro agent may cause your system to reboot. Trend Micro is currently researching this issue.

 Before you begin, Armor recommends that you pre-installation information, including firewall rules.

To learn more, see [Requirements for Armor Anywhere](#).

 Before you install the Armor Anywhere agent, you must remove any previously installed anti-virus software, such as Trend Micro, McAfee, etc. Afterwards, you must reboot your system.

Error rendering macro 'excerpt-include'

No link could be created for 'Complete your account signup (snippet) '.

Step 4: Locate the Armor Anywhere agent

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Virtual Machines**.
3. Click **Deploy New Armor Agent** or click the plus (+) icon.
4. Copy your license key. You will need this information in a later step.
5. Select your operating system (**Windows** or **Linux**).



For Amazon Web Services users who:

- Use **Elastic Beanstalk** to run their instance's applications, and
- Run **Windows 2012 R2**,

Review the following example to understand how to install the Anywhere agent. Afterwards, you can skip to the **Test your connection** step.

```
files:
  "c:\\Windows\\Temp\\armor-setup.exe":
    source: https://get.core.armor.com/latest/armor-setup.exe
commands:
  armoragentinstall:
    test: if not exist 'c:\\.armor\\opt\\armor.exe' exit 0
    command: c:\\Windows\\Temp\\armor-setup.exe /verysilent /license=AAAA1-A11AA-AA1AA-AAAAA-1AAA
    ignoreErrors: false
    waitAfterCompletion: 5
```




You must replace **AAAA1-A11AA-AA1AA-AAAAA-1AAA** with your specific license key.

Step 5: Download and install the Armor Anywhere agent

There are three types of scripts that you can use to install the agent.

Script type	Description
Pre-installation	<p>You can use these scripts to verify that your environment is compatible with Armor Anywhere. These scripts will not install the agent.</p> <pre>[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-WebRequest https://get.core.armor.com/latest/armor_agent.ps1 -outfile armor_agent.ps1 ; .\armor_agent.ps1</pre>
Pre-installation and installation	<p>You can use these scripts to:</p> <ul style="list-style-type: none">• Verify that your environment is compatible with Armor Anywhere• Install the agent <pre>[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-WebRequest https://get.core.armor.com/latest/armor_agent.ps1 -outfile armor_agent.ps1 ; .\armor_agent.ps1 -license AAAA1-A11AA-AA1AA-AAAAA-1AAA</pre>


Installation	<p>You can use these scripts to install the agent. These scripts will not verify your environment for compatibility.</p> <pre>[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-WebRequest https://get.core.armor.com/latest/armor_agent.ps1 -outfile armor_agent.ps1 ; .\armor_agent.ps1 -license AAAA1-A11AA-AA1AA-AAAAA-1AAA -silent</pre>
--------------	---

 In the above scripts, replace **AAAA1-A11AA-AA1AA-AAAAA-1AAA** with your specific license key.

Step 6: Test your connection

After you install the agent, Armor recommends that you test the connection for each configured firewall rule.

To verify connectivity to an Armor service endpoint, use the telnet command.

 The following example tests connectivity to api.armor.com over 443/tcp: Troubleshooting:

```
telnet 146.88.106.210 443
```

For Windows systems without the telnet feature installed, you can also use PowerShell:


```
new-object System.Net.Sockets.TcpClient('146.88.106.210', 443)
```

Step 7: Review the status of the Armor Anywhere agent

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Virtual Machines**.
3. Review the corresponding **Status** column. The **Status** column contains a green or red status to indicate if the server's agent has registered a heartbeat to Armor.
 - A green status indicates the server's agent has registered a heartbeat in the past hour.
 - A red status indicates the server's agent has not registered a heartbeat in the past hour.
 - After four hours without a registered heartbeat, the API will close all service endpoints (firewall ports).


Step 8: Configure your 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 #f0e68c; 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.

Step 9: (For Account Administrators) Create a role and add permissions

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 certain permissions. For example, you can create an **Audit** role, and then you can add specific permissions that will give the assigned user permission to access audit-related features.

By default, a new administrator account contains an **Admin** role with all the available permissions selected.

When you create a new user account, you must assign that user a role. You can assign a default role or create a new role.



There are three default permissions in AMP:

- **Admin** contains every permission in AMP.
- **Technical** contains mostly write-only permissions.
- **Billing** contains mostly read-only permissions.

If you want to use a default role, then you can skip to **Step 8: Create a user and assign a role**.

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 10: (For Account Administrators) Create a user and assign a role

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](#).



Repeat **Step 10: Create a user and assign a role** for every user you want to invite.
